DOCKET NO.: 260977US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Sung Yoon KIM, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP04/08178

INTERNATIONAL FILING DATE: June 4, 2004

FOR: INFORMATION DEVICE, INFORMATION SERVER, INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD AND INFORMATION PROCESSING PROGRAM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2003-163968	09 June 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/08178.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

PCT/JP2004/008178

04. 6. 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月　９日

出願番号
Application Number: 特願２００３－１６３９６８

[ST. 10/C]: [ＪＰ２００３－１６３９６８]

出願人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年　３月　３日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０１６３３８

【書類名】　特許願
【整理番号】　0390168806
【提出日】　平成15年 6月 9日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 07/00
G09C 01/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　金　成潤
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　土屋　健一
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代理人】
【識別番号】　100098785
【弁理士】
【氏名又は名称】　藤島　洋一郎
【手数料の表示】
【予納台帳番号】　019482
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9708092

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　情報機器、情報サーバ、情報処理システム、情報処理方法および情報処理プログラム

【特許請求の範囲】

【請求項１】　暗号化されて配布され、ライセンスの保持を条件として利用可能になるコンテンツを記憶する第１の記憶手段と、

ライセンスを記憶する第２の記憶手段と、

コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶する第３の記憶手段と、

前記第２および第３の記憶手段の記憶内容に基づいて、前記第１の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段と

を備えたことを特徴とする情報機器。

【請求項２】　前記第１の記憶手段は、前記コンテンツの利用を可能にするライセンスを識別するためのライセンス識別情報を、このコンテンツに対応付けて記憶しており、

前記第２の記憶手段に記憶されたライセンスは、前記ライセンス識別情報と前記グループ化機器識別情報とを含んでいる

ことを特徴とする請求項１に記載の情報機器。

【請求項３】　前記再生処理手段は、

再生要求がなされたコンテンツに対応するライセンス識別情報を前記第１の記憶手段から読み出し、

読み出されたライセンス識別情報に対応するグループ化機器識別情報を前記第２の記憶手段から読み出し、

読み出されたグループ化機器識別情報に対応する鍵情報を前記第３の記憶手段から読み出し、

読み出された鍵情報を用いて、前記第１の記憶手段に記憶されたコンテンツを解読して出力する

ことを特徴とする請求項２に記載の情報機器。

【請求項４】　前記情報サーバに対し、自己の属する機器グループを情報サーバに登録することを要求するグループ登録要求を行うグループ登録要求手段とを備えたことを特徴とする請求項１に記載の情報機器。

【請求項５】　前記情報サーバに対して、その情報機器をサービス提供対象として登録し前記グループ化機器識別情報および前記鍵情報を送付することを要求するサービス登録要求を行うサービス登録要求手段

を備えたことを特徴とする請求項４に記載の情報機器。

【請求項６】　自己を他から識別するための固有の機器識別情報を記憶する第４の記憶手段と、

前記情報サーバに対して、前記第４の記憶手段に記憶された機器識別情報を情報サーバに登録することを要求する機器登録要求を行う機器登録要求手段と

を備えたことを特徴とする請求項４に記載の情報機器。

【請求項７】　前記第４の記憶手段に記憶されるべき前記機器識別情報を生成する機器識別情報生成手段を備えたことを特徴とする請求項６に記載の情報機器。

【請求項８】　前記情報サーバに対して、前記第４の記憶手段に記憶された機器識別情報を情報サーバの登録から削除することを要求する機器登録削除要求を行う機器登録削除要求手段を備えたことを特徴とする請求項６に記載の情報機器。

【請求項９】　１つの機器グループが、１のユーザの保有する複数の情報機器からなるグループとして規定されている

ことを特徴とする請求項１に記載の情報機器。

【請求項１０】　前記鍵情報は、最上層から最下層に向かって枝分かれしていく階層ツリー構造における各ノードに対応して規定され暗号化されたノードキーのうち、最下層のデバイスノードとしての自機器グループに割り当てられたデバイスノードキーに該当するものであり、

前記コンテンツは、前記階層ツリー構造における前記デバイスノードキーから最上層のノードキーであるルートキーに至る経路上の各ノードキーを用いて多重

に暗号化されたものであり、

前記再生処理手段は、デバイスノードキーとしての前記鍵情報を用いて、前記階層ツリー構造における最下層から最上層に至る経路上のノードキーを順次解読し、得られた前記ルートキーを用いて前記コンテンツを解読する

ことを特徴とする請求項１に記載の情報機器。

【請求項１１】　前記コンテンツは、さらに、前記ルートキーによって暗号化されたコンテンツキーを用いて暗号化されており、

前記再生処理手段は、さらに、前記ルートキーによって前記コンテンツキーを解読し、得られたコンテンツキーを用いて前記コンテンツを解読する

ことを特徴とする請求項１０に記載の情報機器。

【請求項１２】　前記コンテンツは、テキストデータ、静止画像データ、動画像データ、音声データ、またはそれらを組み合わせてなるデータである

ことを特徴とする請求項１に記載の情報機器。

【請求項１３】　暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバであって、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する機器グループ内の複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与するサービス登録処理手段と

を備えたことを特徴とする情報サーバ。

【請求項１４】　前記情報機器からの機器登録要求に応じて、その機器登録要求から、個々の情報機器を識別するための機器識別情報を抽出し、この機器識別情報を前記グループ識別子に対応付けて登録する機器登録管理手段と

を備えたことを特徴とする請求項１３に記載の情報サーバ。

【請求項１５】　前記機器登録管理手段は、一の機器グループについて登録された機器識別情報の数が一定数に達した以降は、その機器グループに属する新たな情報機器からの機器登録要求を拒否する

ことを特徴とする請求項１４に記載の情報サーバ。

【請求項１６】　前記機器登録管理手段は、前記情報機器からの機器登録削除要求に応じて、この機器登録削除要求により指定された機器識別情報を登録から削除する

ことを特徴とする請求項１４に記載の情報サーバ。

【請求項１７】　情報機器からのライセンス要求に応じて、このライセンス要求によって指定されたライセンスを、そのライセンス要求をしてきた情報機器に提供するライセンス提供手段と、

前記ライセンス要求からグループ化機器識別情報を抽出し、その抽出されたグループ化機器識別情報が前記サービス登録処理手段によって登録されたものであるか否かを調べ、その結果に応じて、前記ライセンス提供手段によるライセンス提供に伴う課金処理を行うか否かを判定する課金処理手段と

を備えたことを特徴とする請求項１３に記載の情報サーバ。

【請求項１８】　１つの機器グループが、１のユーザの保有する複数の情報機器からなるグループとして規定されている

ことを特徴とする請求項１３に記載の情報サーバ。

【請求項１９】　暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバと、この情報サーバから通信回線を通じてサービスを受けるクライアントとしての情報機器とを含んで構成される情報処理システムであって、

前記情報サーバは、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化

して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与するサービス登録処理手段と

を備え、

前記情報機器は、

コンテンツを記憶する第１の記憶手段と、

ライセンスを記憶する第２の記憶手段と、

前記情報サーバから付与された前記グループ化機器識別情報と前記鍵情報とを、前記グループ識別子と共に記憶する第３の記憶手段と、

前記第２および第３の記憶手段の記憶内容に基づいて、前記第１の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段と

を備えたことを特徴とする情報処理システム。

【請求項２０】　暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバと、前記情報サーバからサービスを受けるクライアントとしての情報機器とを含む情報処理システムに適用される情報処理方法であって、

前記情報サーバにおいて、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録し、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与し、

前記情報機器において、

コンテンツとライセンスとを記憶し、

前記情報サーバから付与された前記グループ化機器識別情報と前記鍵情報とを

、前記グループ識別子と共に記憶し、

記憶されている前記ライセンスの内容と前記グループ化機器識別情報と前記鍵情報とに基づいて、記憶されている前記コンテンツを解読して再生する処理を行う

ことを特徴とする情報処理方法。

【請求項２１】　コンテンツを利用する機能を備えた情報機器に適用されるプログラムであって、

暗号化されて配布されライセンスの保持を条件として利用可能になるコンテンツを記憶するステップと、

ライセンスを記憶するステップと、

コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶するステップと、

前記第２および第３の記憶手段の記憶内容に基づいて、前記第１の記憶手段に記憶されたコンテンツを解読して再生する処理を行うステップと

を前記情報機器に実行させることを特徴とする情報処理プログラム。

【請求項２２】　暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバに適用されるプログラムであって、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するステップと、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与するステップと

を前記情報サーバに実行させることを特徴とする情報処理プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツを利用する機能を備えた情報機器、コンテンツの利用を許可するライセンスを発行する情報サーバ、そのような情報機器および情報サーバを含む情報処理システム、そのような情報処理システムに適用される情報処理方法、ならびにそのような情報機器および情報サーバに適用されるプログラムに関する。

【０００２】

【従来の技術】

近年、ユーザが、ＰＣ（Personal Computer）を利用してインターネット経由で自分自身が保持している音楽データ等のコンテンツを他のユーザに提供する一方、自分自身が保持していないコンテンツを他のユーザから提供してもらうという、コンテンツ交換システムが出現している。

【０００３】

この種のシステムでは、理論的には、１つのコンテンツが存在すれば、他のすべてのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなる。その結果、そのコンテンツの著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴って本来受け取ることが可能なロイヤリティを受け取る機会を失うことになる。そこで、コンテンツの流通を妨げることなく、著作権者からライセンスを受けていないコンテンツが不正にコピーされて利用されることを防止することが社会的に要請されている。

【０００４】

そのような要請に応じて、例えば下記の特許文献１に記載されているように、コンテンツの配布を自由に行うことができると共に、許可されたユーザのみがコンテンツを利用できるようにした、いわゆるＯｐｅｎＭＧＸ（商標）と呼ばれる技術が提案されている。

【０００５】

この技術は、次のようなものである。クライアントは、暗号化されたコンテン

ツをコンテンツサーバから受け取る。コンテンツのヘッダには、そのコンテンツを利用するとき必要とされるライセンスを特定するためのライセンス特定情報が記述されている。クライアントは、ライセンス特定情報に基づいて、ライセンスサーバにライセンスを要求する。ライセンスサーバは、ライセンス要求を受け取ると、課金処理を行った後、該当するライセンスをクライアントに送信する。クライアントはライセンスを保持していることを条件として、コンテンツを復号し再生することができる。この技術によれば、コンテンツの配布を自由に行うことができる一方、許可されたユーザのみがコンテンツを利用できることとなるため、コンテンツの不正利用を防止しつつコンテンツの流通を促進することが可能である。

【０００６】

【特許文献１】

特開２００２－３５９６１６号公報

【０００７】

【発明が解決しようとする課題】

近年のインターネットの爆発的な普及と急速なブロードバンド化とにより、ＰＣだけではなく、いわゆるＣＥ機器（Consumer Erectronics）と呼ばれる家電向け電子機器もまた直接ネットワークに繋がることになることが予測される。また、１人で複数のＰＣやネットアクセス可能なＣＥ機器を持つようになると考えられる。

【０００８】

しかしながら、このように、個人が持つ複数の機器がネットワークに接続されるようになった場合、従来のようにコンテンツやライセンスをダウンロードした１つの機器でのみ一元管理するモデルでは、ユーザの使い勝手が悪くなる。例えば、あるユーザがあるコンテンツを自宅のＰＣでネットワークを介して購入したとする。そのコンテンツを外出先でポータブル機器により利用したいと考えたとき、もう一度そのコンテンツを購入せざるを得ない。

【０００９】

本発明はかかる問題点に鑑みてなされたもので、その目的は、コンテンツを正

当な手段で入手したユーザのみが再生可能となるように保護されたコンテンツをユーザが自己の情報機器によって取得した場合に、そのコンテンツを、そのユーザが所有する他の情報機器でも利用することが可能となるような情報機器、情報サーバ、情報処理システム、情報処理方法および情報処理プログラムを提供することにある。

【００１０】

【課題を解決するための手段】

本発明の情報機器は、暗号化されて配布され、ライセンスの保持を条件として利用可能になるコンテンツを記憶する第１の記憶手段と、ライセンスを記憶する第２の記憶手段と、コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶する第３の記憶手段と、第２および第３の記憶手段の記憶内容に基づいて、第１の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段とを備えている。

【００１１】

本発明の情報サーバは、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する機器グループ内の複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するサービス登録処理手段とを備えている。

【００１２】

本発明の情報処理方法は、情報サーバの側において、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録し、情報機器からのサー

ビス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与し、情報機器の側において、コンテンツとライセンスとを記憶し、情報サーバから付与されたグループ化機器識別情報と鍵情報とを、グループ識別子と共に記憶し、記憶されているライセンスの内容とグループ化機器識別情報と鍵情報とに基づいて、記憶されているコンテンツを解読して再生する処理を行うようにしたものである。

【００１３】

本発明の情報処理システムは、情報サーバと情報機器とを含んで構成される。情報サーバは、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するサービス登録処理手段とを備え、情報機器は、コンテンツを記憶する第１の記憶手段と、ライセンスを記憶する第２の記憶手段と、情報サーバから付与されたグループ化機器識別情報と鍵情報とを、グループ識別子と共に記憶する第３の記憶手段と、第２および第３の記憶手段の記憶内容に基づいて、第１の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段とを備えている。

【００１４】

本発明の第１の情報処理プログラムは、暗号化されて配布されライセンスの保持を条件として利用可能になるコンテンツを記憶するステップと、ライセンスを記憶するステップと、コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付

与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶するステップと、第２および第３の記憶手段の記憶内容に基づいて、第１の記憶手段に記憶されたコンテンツを解読して再生する処理を行うステップとを情報機器に実行させるものである。

【００１５】

本発明の第２の情報処理プログラムは、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するステップと、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するステップとを情報サーバに実行させるものである。

【００１６】

本発明の情報機器または第１の情報処理プログラムでは、コンテンツとライセンスとが記憶されると共に、グループ化機器識別情報とコンテンツ解読用の鍵情報とがグループ識別子と共に記憶される。ライセンスに含まれる情報と、グループ化機器識別情報と、コンテンツ解読用の鍵情報と、グループ識別子とに基づいて、コンテンツが解読されて再生され、利用可能になる。

【００１７】

本発明の情報サーバまたは第２の情報処理プログラムでは、情報機器からのグループ登録要求に応じてグループ登録処理が行われ、情報機器からのサービス登録要求に応じてサービス登録処理が行われる。グループ登録処理においては、登録対象の機器グループに関する情報がグループ識別子に対応付けられて登録される。サービス登録処理においては、登録を要求してきた情報機器が、サービス提供対象として登録される。また、サービス登録処理においては、一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とが、上記のグループ識別子に対応付けられて登録される。さらに、サービス登録処理においては、登録を要求し

てきた情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とが付与される。この結果、その機器グループ内のすべての情報機器が、同じグループ化機器識別情報および鍵情報をもつことになる。

【００１８】

本発明の情報処理システムまたは情報処理方法では、上記の情報機器または第１の情報処理プログラムの作用と、上記の情報サーバまたは第２の情報処理プログラムの作用の双方が具現化される。すなわち、１つの機器グループ内のすべての情報機器が同じグループ化機器識別情報および鍵情報をもつことになると共に、各情報機器においては、コンテンツが解読されて再生され、利用可能になる。

【００１９】

なお、本明細書において用いる用語の基本的意義は、以下の通りである。

【００２０】

「コンテンツ」とは、ディジタル化され暗号化されて配布されたコンテンツ本体部分をいい、テキスト情報、静止画や動画等の画像情報、音声情報、およびそれらの組み合わせ等をいう。例えば、電子書籍や電子新聞等のようなテキスト情報と画像情報とを組み合わせたものや、ゲームプログラムのようなアプリケーションソフトウェア等も含む。配布の形態は問わず、インターネット等の通信回線を介してにより配信されたものでも、ＣＤ－ＲＯＭ等の記録媒体によって配布されたものでも構わない。「コンテンツの利用」とは、凡そコンテンツが有する情報を役立つ（意味のある）形で用いることをいい、コンテンツを再生し、閲覧し、または実行する行為等を含む。

【００２１】

「情報機器」とは、専用のコンテンツ利用機器のほか、パーソナルコンピュータ（ＰＣ）等のような汎用のコンピュータも含む。以下の説明では、単に「機器」または「デバイス」ともいう。「情報サーバ」とは、ライセンスを提供するための装置をいい、広くワークステーションやＰＣ等の情報処理装置を含む。

【００２２】

「ライセンス」とは、コンテンツの利用を可能ならしめるための利用権情報で

あり、利用条件を含むほか、それ自体を識別するためのライセンス識別情報等も含む。「機器グループ」とは、一群の情報機器をいう。一般的には、１ユーザが保有する複数の情報機器群に該当するが、必ずしもこれに限定されない。

【００２３】

「グループ化機器識別情報」とは、グループ分けされた個々の情報機器がどの機器グループに属するかを示す、いわばグローバルな次元での（機器グループ間での）機器識別情報である。言い換えると、ある機器グループに属することを表示するために各情報機器に付与される情報である。したがって、ある１つの機器グループ内においては、すべての情報機器が同じグループ化機器識別情報をもつ。この情報は、ユーザからは認識できないセキュアな情報として取り扱われるので、通常のユーザにとっては、機器グループの内外を問わず情報機器間で移動やコピーをしたり、情報自体の改変を行うことはできない。以下の実施の形態では、リーフＩＤがその一具体例に対応する。

【００２４】

「グループ識別子」とは、機器グループを形成するときに、便宜的に機器グループごとに付与される一種のラベル情報であり、ユーザから認識できる。既存の機器グループに情報機器を追加登録する際に利用される。ユーザ＝機器グループと考えたときには、一種のユーザ識別情報に相当する。以下の実施の形態では、グループＩＤがその一具体例に対応する。

【００２５】

「機器識別情報」とは、１つの機器グループ内において個々の情報機器を識別するために用いられる、いわばローカルな次元での（機器グループ内での）機器識別情報である。製造や販売の段階で情報機器自体に最初から設定される場合のほか、乱数等を用いたソフトウェアによってあとから生成される場合もある。以下の実施の形態では、機器ＩＤがその一具体例に対応する。

【００２６】

「鍵情報」とは、暗号化されたコンテンツを解読した利用可能な状態にするための解読（復号）用のキーである。本発明では、機器グループごとに共通のキーが付与される。したがって、１つの機器グループ内においては、すべての情報機

器が同じキーをもつ。このキーは、ユーザからは認識できないセキュアな情報として取り扱われるので、通常のユーザにとっては、機器グループの内外を問わず情報機器間で移動やコピーをしたり、情報自体の改変を行うことはできない。以下の実施の形態では、デバイスノードキーＤＮＫがその一具体例に対応する。

【００２７】

「課金処理」とは、ライセンスの販売に対する対価を徴収するために必要な手続き（例えば、銀行決済のための手続き）をいう。

【００２８】

「１のユーザ」…一般的には一個人としてのユーザを指すが、必ずしもこれに限定されない。ライセンサーが許容するのであれば、例えば、生計を共にする１つの家族全体や、１つの社会的組織を指すこともある。

【００２９】

「ノード」は、枝分かれする地点（分岐点）のことであり、「ノードキー」は各ノードごとに設定される暗号化キーであり、直下のノードキーによって暗号化されている。「デバイスノード」とは、最下層のデバイス（本発明では機器グループ）に対応するノードをいい、「デバイスノードキー」とは、最下層のデバイスに対応して規定される暗号化キーであり、上記の「鍵情報」と同義である。本発明では、１つの機器グループ内の情報機器には同じデバイスノードキーが付与される。「ルートキー」とは、階層ツリー構造の頂点に位置する暗号化キーである。

【００３０】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して詳細に説明する。

【００３１】

図１は、本発明の一実施の形態に係る情報機器および情報サーバを含む情報処理システムの全体構成を表すものである。なお、本発明の実施の形態に係る情報処理方法およびプログラムは、本実施の形態の情報処理システムによって具現化されるので、以下、併せて説明する。

【００３２】

この情報処理システムは、コンテンツを利用するクライアントとしての情報機器１－１～１－４と、情報サーバ４とを含んで構成されたコンテンツ配信利用システムである。これらの情報機器１－１～１－４および情報サーバ４は、いずれもインターネット２に接続されている。情報サーバ４は、暗号化されたコンテンツを情報機器１－１～１－４に提供するコンテンツ提供機能と、提供されたコンテンツを利用するのに必要なライセンスを情報機器１に付与するライセンス提供機能と、情報機器１－１～１－４がこのコンテンツ配信利用サービスを受ける際にまず必要となるサービス登録（ユーザ登録）を行うサービス登録機能と、情報機器がライセンスを受け取った場合に、その情報機器に対して課金処理を行う課金機能とを備えている。サービス登録機能およびライセンス提供機能は、例えば、「ＯｐｅｎＭＧＸ」と呼ばれる著作権管理技術を用いて実現することができる。

【００３３】

情報機器１－１～１－４のうち、情報機器１－１～１－３は、あるユーザが所有する情報機器群であり、１つの機器グループ１Ｇを構成している。一方、情報機器１－４は他のユーザの所有するものである。情報機器１－１～１－４は、コンテンツ再生機能を有する専用の機器であってもよいし、あるいは汎用のＰＣであってもよい。なお、以下の説明では、１つの情報機器は１つの機器グループにのみ所属するものとし、１つの情報機器が複数の機器グループに跨がって所属することはないものとする。

【００３４】

情報機器１－１～１－３は、所定の事前手続き（後述）を行うことにより、同一の機器グループ１Ｇに属するようになり、コンテンツおよびライセンスを相互に移動させてコンテンツおよびライセンスを利用することが可能である。情報機器１－４は機器グループ１Ｇに属していないので、コンテンツおよびライセンスを情報機器１－１～１－３から入手しても利用可能とはならない。同様に、情報機器１－４のコンテンツおよびライセンスを情報機器１－１～１－３が入手したとしても、利用可能とはならない。

【００３５】

なお、この図の例においては、情報機器が４台のみ示されているが、実際には、任意の台数の情報機器がインターネット２に接続される。また、機器グループ１Ｇは３台の情報機器を含んでいるが、実際には任意の台数を含んでいてよい。また、この図では、１つの機器グループのみを示しているが、実際には、複数の機器グループが存在し得る。

【００３６】

機器グループ１Ｇに含まれる各情報機器１－１～１－３は、それらの物理的同一性を問題とする立場に立った場合の情報サーバ４からすると、互いに別々のハードウェアであると認識されるが、コンテンツ利用ライセンスの有効性を管理する立場に立った場合の情報サーバ４からすると、コンテンツの利用を許可された互いに区別されない（個性のない）情報機器であると認識されるようになっている。上記の物理的同一性は、各情報機器１－１～１－３がそれぞれ有する固有の機器識別情報（機器ＩＤ）に基づいて判断される。

【００３７】

一方、上記のライセンスの有効性は、予め情報情報サーバ４から情報機器１－１～１－３にそれぞれ付与されるグループ化機器識別情報（以下、リーフＩＤともいう。）および鍵情報ＤＮＫ（デバイスノードキー；Device Node Key）に基づいて判断され、管理される。すなわち、１つの機器グループ内の情報機器は、それぞれ、互いに異なる（少なくともその機器グループ内で重複しない）機器ＩＤを有する一方、同一の（共通の）リーフＩＤと同一の（共通の）鍵情報ＤＮＫとを有する。これらのリーフＩＤおよび鍵情報ＤＮＫは、ユーザからは不可視（認識不可能）であるようにセキュアな情報として取り扱われるので、機器グループの内外を問わず、情報機器間での移動やコピーはできない。また、ユーザ自身はリーフＩＤを認識できないので、ユーザがなすべき各種の登録手続き等を可能ならしめるために、機器グループごとに、ユーザＩＤでもあるグループ識別子（グループＩＤ）が付与されて、運用されるようになっている。なお、機器ＩＤ、リーフＩＤ、鍵情報ＤＮＫおよびグループＩＤについての詳細は後述する（図５、図６）。

【００３８】

図２は情報機器１－１の一構成例を表すものである。

【００３９】

図２に示したように、情報機器１－１は、ＣＰＵ（Central ProcessingUnit）２１と、ＲＯＭ（Read Only Memory）２２と、ＲＡＭ（Random Access Memory）２３と、暗号化復号部２４と、コーデック部２５と、入出力インタフェース３２とを備えている。これらは、バス３１を介して相互に接続されている。このバス３１にはまた、入出力インタフェース３２を介して、入力部２６と、出力部２７と、記憶部２８と、通信部２９と、ドライブ３０とが接続されている。

【００４０】

ＣＰＵ２１は、ＲＯＭ２２に記憶されているプログラム、または記憶部２８からＲＡＭ２３にロードされたプログラムに従って各種の処理を実行する。タイマ２０は、計時動作を行い、時刻情報をＣＰＵ２１に供給する。ＲＡＭ２３には、ＣＰＵ２１が各種の処理を実行する上において必要なデータ等も適宜記憶される。

【００４１】

暗号化復号部２４は、既に暗号化されているコンテンツを解読（復号）する処理を行うためのものである。但し、後述するように、図２の構成が情報サーバ４に適用される場合には、暗号化復号部２４はコンテンツを暗号化する機能を有する。コーデック部２５は、例えば、ＡＴＲＡＣ（Adaptive Transform Acoustic Coding）３方式などで音楽コンテンツを圧縮（エンコード）して入出力インタフェース３２に出力したり、逆に、入出力インタフェース３２から入力され暗号化復号部２４で解読された圧縮コンテンツを、再生可能なデータへと伸長（デコード）するためのものである。

【００４２】

入力部２６は、キーボードやマウス等よりなり、出力部２７は、ＣＲＴ（陰極線管）、ＬＣＤ（液晶表示装置）等のディスプレイや、スピーカ等よりなる。記憶部２８は、ハードディスク等により構成され、コンテンツやライセンスのほか、各種の管理情報を記憶する。通信部２９は、モデムやターミナルアダプタ等より構成され、インターネット２を介して通信処理を行う機能を有する。具体的に

は、通信部２９は、情報サーバ４に接続して暗号化されたコンテンツをダウンロードしたり、情報サーバ４と接続してライセンスのダウンロードや各種の登録手続き（後述）のための通信処理を行う。

【００４３】

ドライブ３０には、例えば、リムーバブルな磁気ディスク４１、光ディスク４２、光磁気ディスク４３、あるいは半導体メモリ４４等の記憶媒体が着脱可能に装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされるようになっている。ドライブ３０はまた、これらの記憶媒体からコンテンツを読み取ったり、逆に、これらの記憶媒体にコンテンツを記録する処理を行う場合もある。なお、光ディスク４２には、ＣＤ－ＲＯＭ（CompactDisk-Read Only Memory）、ＣＤ－Ｒ(Recordable)、ＣＤ－ＲＷ(ReWritable)、ＤＶＤ（DigitalVersatileDisk）－ＲＯＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ等が含まれ、半導体メモリ４４は、例えば、メモリスティック（商標）等により構成される。

【００４４】

なお、他の情報機器１－２～１－４についても、図２に示した情報機器１－１と同じハードウェア構成を有する。また、図示は省略するが、情報サーバ４もまた、図２に示した情報機器１－１と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、必要に応じて、図２の構成を、情報サーバ４の構成としても引用するものとする。

【００４５】

図３は、情報機器１－１の機能構成を表すものであり、本実施の形態におけるクライアント用の情報処理プログラムの基本構成に相当する。情報機器１－１の機能は、制御機能ブロック５０と、通信機能ブロック７０と、記憶機能ブロック８０とに大別される。制御機能ブロック５０は、再生処理機能５１と、グループ登録要求機能５２と、機器登録要求機能５３と、サービス登録要求機能５４と、機器登録削除要求機能５５と、機器ＩＤ生成機能５６と、コンテンツ・ライセンス要求機能５７とを含む。記憶機能ブロック８０は、第１の記憶部８１～第４の記憶部８４を含む。

【００４６】

制御機能ブロック５０の各機能は主として図２のＣＰＵ２１や暗号化復号部２４等が担当する。通信機能ブロック７０は主として図２の通信部２９が担当し、記憶機能ブロック８０の各機能は主として図２の記憶部２８やＲＡＭ２３が担当する。

【００４７】

制御機能ブロック５０の各機能の具体的内容は次の通りである。

【００４８】

再生処理機能５１は、第２の記憶部８２および第３の記憶部８３の記憶内容に基づいて、第１の記憶部８１に記憶されたコンテンツを解読して再生するものである。グループ登録要求機能５２は、情報サーバ４に対し、自機器（情報機器１－１）が属する機器グループを情報サーバ４に登録することを要求するグループ登録要求を行う機能である。機器登録要求機能５３は、情報サーバ４に対し、第４の記憶部８４に記憶された機器ＩＤを情報サーバ４に登録することを要求する機器登録要求を行う機能である。サービス登録要求機能５４は、情報サーバ４に対し、自機器をサービス提供対象として登録しリーフＩＤおよび鍵情報ＤＮＫを送付することを要求する機能である。機器登録削除要求機能５５は、情報サーバ４に対して、第４の記憶部８４に記憶された機器ＩＤを情報サーバ４の登録から削除することを要求する機器登録削除要求を行う機能である。機器ＩＤ生成機能５６は、機器登録要求機能５３が必要とする機器ＩＤを生成して、第４の記憶部８４に記憶させる機能である。コンテンツ・ライセンス要求機能５７は、情報サーバ４に対して、コンテンツやライセンスのダウンロードを要求する機能である。

【００４９】

記憶機能ブロック８０の各機能の内容は次の通りである。

【００５０】

第１の記憶部８１は情報サーバ４等から提供されたコンテンツを記憶する機能を有し、第２の記憶部８２は情報サーバから提供されたライセンスを記憶する機能を有する。第３の記憶部８３は、複数の情報機器をグループ化して識別するた

めのリーフＩＤと機器グループごとに共通に付与されたコンテンツ解読用の鍵情報ＤＮＫとを、機器グループごとに付与されたグループＩＤと共に記憶する機能である。図１の例では、リーフＩＤおよび鍵情報ＤＮＫは、ひとつのグループＩＤをもつ機器グループ１Ｇに含まれる情報機器１－１～１－３について共通化されたものである。第４の記憶部８４は、自機器（情報機器１－１）を機器グループ１Ｇ内の他の情報機器１－２，１－３から識別するための固有の機器ＩＤを記憶する機能を有する。

【００５１】

図４は、情報サーバ４の機能構成を表すものであり、本実施の形態におけるサーバ用の情報処理プログラムの基本構成に相当する。情報サーバ４の機能は、制御機能ブロック９０と、通信機能ブロック１００と、記憶機能ブロック１１０とに大別される。制御機能ブロック９０は、コンテンツ・ライセンス提供機能９４と、グループ登録処理機能９１と、機器登録管理機能９２と、サービス登録処理機能９３と、課金処理機能９５とを含む。記憶機能ブロック１１０は、コンテンツ蓄積部１１１と、ライセンステーブル１１２と、グループ管理テーブル１１３とを含む。

【００５２】

制御機能ブロック９０の各機能は主としてＣＰＵ２１や暗号化復号化部２４等が担当し、通信機能ブロック１００は主として通信部２９が担当し、記憶機能ブロック１１０は主として記憶部２８やＲＡＭ２３が担当する。

【００５３】

制御機能ブロック５０の各機能の具体的内容は次の通りである。

【００５４】

コンテンツ・ライセンス提供機能９４は、リーフＩＤを含むコンテンツ要求やライセンス要求を情報機器１－１等から受け付け、その要求されたコンテンツやライセンスを、その要求をしてきた情報機器に提供する機能である。

【００５５】

グループ登録処理機能９１は、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報

（グループ情報）をグループ識別子に対応付けて登録する機能である。

【００５６】

機器登録管理機能９２は、情報機器からの機器登録要求に応じて、その機器登録要求から、個々の情報機器を識別するための機器識別情報を抽出し、この機器識別情報をグループ識別子に対応付けて登録する処理を行うほか、情報機器からの機器登録削除要求に応じて、この機器登録削除要求により指定された機器識別情報を登録から削除する処理を行う機能である。機器登録管理機能９２はまた、ある機器グループについて登録された機器ＩＤの数が一定数に達した以降は、新たな情報機器からの機器登録要求を拒否する処理を行う機能も含む。

【００５７】

サービス登録処理機能９３は、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、リーフＩＤおよび鍵情報ＤＮＫをグループＩＤに対応付けてグループ管理テーブル１１３に登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、その登録されたリーフＩＤおよび鍵情報ＤＮＫを付与する機能である。このサービス登録機能９３は、本実施の形態では、「ＯｐｅｎＭＧＸ」登録処理が相当する。

【００５８】

課金処理機能９５は、情報機器よりなされたライセンス要求からリーフＩＤを抽出し、その抽出されたリーフＩＤがグループ登録機能により登録されているか否かを調べ、その結果に応じて、コンテンツ・ライセンス提供機能９４によるライセンス提供に伴う課金処理を行うか否かを判定する機能である。

【００５９】

記憶機能ブロック１１０の各機能の具体的内容は次の通りである。

【００６０】

コンテンツ蓄積部１１１は、情報機器からの要求に応じて提供する多種多様なコンテンツを予め作成して蓄積するものである。ライセンステーブル１１２は、例えば図５（Ｂ）に示したように、各コンテンツに対応して用意されたライセンスのリストテーブルである。グループ管理テーブル１１３は、図５（Ａ）に示したように、リーフＩＤと鍵情報ＤＮＫとをグループＩＤに対応付けて登録すると

共に、機器ＩＤをリーフＩＤに対応付けて登録するものである。ライセンステーブル１１２およびグループ管理テーブル１１３については以下に詳述する。

【００６１】

図５（Ａ）は、グループ管理テーブル１１３の一例を表すものである。このグループ管理テーブル１１３には、グループＩＤ１２１に対応して、パスワード１２２と、グループ情報１２３と、機器ＩＤ１２４と、サービスデータ１２５とが互いに対応付けられて登録されている。なお、この図では、後述するトランザクションＩＤ（ＴＩＤ）の図示を省略している。ここで、グループＩＤ：パスワード：機器ＩＤ：サービスデータの対応関係は、１：１：ｎ：１である。但し、ｎは正の整数である。

【００６２】

グループＩＤ１２１およびパスワード１２２はグループ登録時に割り当てられ、機器ＩＤ１２４は機器登録時に割り当てられ、サービスデータ１２５はサービス登録時に割り当てられるようになっている。

【００６３】

ここで、グループ登録とは、ユーザが機器グループ１Ｇによってコンテンツ配信サービスを利用するに当たり、始めに一度だけ行われる登録である。グループ登録を行うことにより、ユーザは、グループＩＤとパスワードとを取得し、これらを用いることにより、コンテンツ配信サービスにおける機器登録やコンテンツの購入等を行うことができるようになる。

【００６４】

また、機器登録とは、あるユーザが所有する１つ以上の機器を１つのグループとしてサーバが管理するための処理である。

【００６５】

サービス登録とは、機器登録の済んだ情報機器を用いてコンテンツを利用するに際して必要となる手続きであり、本来は、個々の情報機器とコンテンツ解読キーとを関連付けることにより、情報機器間での不正コピーによる利用を防止することを目的として行われる処理である。但し、本実施の形態では、グループ登録の済んだ機器グループ内においては、情報機器間でコンテンツやライセンスを自

由にコピーすることが許容される。

【００６６】

なお、グループ登録、機器登録およびサービス登録の詳細は後述する。

【００６７】

グループＩＤ１２１は、その機器グループそのものを特定し、他の機器グループから識別するためのものであり、いずれかの情報機器からのグループ登録要求に応じて、その要求をした情報機器の属する機器グループに付与される。本実施の形態のように、１ユーザが１機器グループに対応するようになっている場合には、このグループＩＤ１２１はユーザＩＤに相当する。パスワード１２２は、グループ登録の際に、グループＩＤ１２１と共に付与される。これらのグループＩＤ１２１およびパスワード１２２は、機器グループを形成するときに、情報サーバ４から便宜的に機器グループごとに付与される情報であり、ユーザからも認識可能である。ユーザは、既登録の機器グループに情報機器を追加登録する場合や機器登録を削除する場合に、入力を求められるようになっている。

【００６８】

グループ情報１２３は、機器グループに関する情報であり、グループ登録時にユーザから提供される。本実施の形態のように、１ユーザが１機器グループに対応する場合には、グループ情報１２３はユーザの個人情報（ユーザの氏名、住所、電話番号、メールアドレス、クレジットカード番号等）に相当する。

【００６９】

機器ＩＤ１２４は、１つの機器グループ内において個々の情報機器を識別するために用いられる、いわばローカルな次元での（機器グループ内での）機器識別情報である。すなわち、機器ＩＤ１２５は、ある機器グループ内の情報機器間で互いに異なるものとなっており、この点で、機器グループ内の情報機器に共通に付与されるリーフＩＤとは異なる。この機器ＩＤ１２５によって、機器グループに何台の情報機器が登録されているかが把握される。この機器ＩＤ１２５は、情報機器１－１が専用のコンテンツ再生機器の場合には、製造や販売の段階でＲＯＭ２２に設定されるが、情報機器１－１がＰＣ等の汎用機の場合には、乱数等を用いたソフトウェアによってあとから（例えば、後述する機器登録時に）生成さ

れる。このようなソフトウェアは、例えばグループ登録時や機器登録時に情報サーバ４からダウンロードされ、図３の機器ＩＤ生成機能５６を実現する。

【００７０】

サービスデータ１２５は、リーフＩＤと鍵情報ＤＮＫとを含む。リーフＩＤは、コンテンツを利用しようとする複数の情報機器をグループ化して識別するために各情報機器に付与される情報であり、上記のように「グループ化機器識別情報」の一具体例に対応する。言い換えると、リーフＩＤは、ある機器グループに属することを表示するために各情報機器に付与される情報である。鍵情報ＤＮＫは、コンテンツ解読用のキーであり、後述する階層ツリー構造（図７）のノードのうち最下層のノードに付与されるリーフキーを含んで構成されたデバイスノードキーである（図８（Ｂ）～（Ｄ）参照）。機器グループごとに共通の鍵情報ＤＮＫが付与される。したがって、１つの機器グループ内においては、すべての情報機器が同じリーフＩＤと鍵情報ＤＮＫとをもつ。これらのリーフＩＤおよび鍵情報ＤＮＫを利用して運用することにより、１つの機器グループ内のすべての情報機器において、（ライセンスされた）コンテンツを自由に利用することが可能になる。なお、リーフＩＤおよび鍵情報ＤＮＫの意義については、後にさらに詳述する。

【００７１】

図５（Ａ）に示した例では、情報機器１－１～１－３からなる機器グループ１Ｇ（図１）に、「G_0」というグループＩＤと「ＡＢＣＤ」というパスワードが付されると共に、「L_0」というリーフＩＤと「DNK_0」という鍵情報ＤＮＫとが付与されている。この例では、機器グループ１Ｇに属する情報機器１－１～１－３が、それぞれ、D_0，D_1，D_2 という機器ＩＤを有するものとして登録されている状態を示している。

【００７２】

図５（Ｂ）は、ライセンステーブル１１２の一例を表すものである。このライセンステーブル１１２には、ライセンスＩＤ１２７と、ライセンスの内容１２８と、ライセンスを付与した機器グループのグループＩＤ１２９とが対応付けられて登録されている。図５（Ｂ）に示した例では、例えば、「ａｂｃｄｅｆ」とい

うライセンスＩＤのライセンスに対して、３つのグループＩＤ（「G_0」，「G_1」，「G_2」）が対応付けられており、これにより、これらのグループＩＤをもつ３つの機器グループにそのライセンスがそれぞれ提供されていることがわかる。

【００７３】

図６は、情報機器１－１の記憶機能ブロック８０（図３）により記憶されている情報の内容を表すものである。具体的には、例えば記憶部２８（図２）の記憶内容である。なお、この図において、下線を付したものはユーザが認識し得る（見える）情報である。また、リーフＩＤや鍵情報ＤＮＫのように下線を付していないものはユーザからは認識できないセキュアな情報であり、ユーザがコピーや移動等の操作をすることはできないようになっている。

【００７４】

記憶機能ブロック８０は、コンテンツファイル１３０と、ライセンス１４０と、ユーザデータ１５０とを記憶する。これらの情報の記憶は、それぞれ、第１の記憶部８１～第３の記憶部８３によって担保されている。

【００７５】

まず、コンテンツファイル１３０について説明する。このコンテンツファイル１３０は、ヘッダ（Header）部分とデータ（Data）部分とにより構成される。ヘッダ部分は、コンテンツ識別情報（コンテンツＩＤ）１３１と、ディジタル権利管理情報（ＤＲＭ；Digital Right Management）１３２と、ライセンス識別情報（ライセンスＩＤ）１３３と、有効化キーブロックＥＫＢ（Enabling Key Block）１３４と、暗号化されたコンテンツキー（以下、被暗号化コンテンツキーともいう。）１３５とを含んで構成されている。データ部分は、暗号化されたコンテンツ（以下、被暗号化コンテンツともいう。）１３６によって構成される。なお、この被暗号化コンテンツ１３６は、複数のブロックに分けて暗号化されている。

【００７６】

コンテンツＩＤ１３１は、コンテンツ自体を特定または識別するための情報である。なお、このコンテンツＩＤ１３１に付随させて、そのコンテンツのコーデ

ック方式等の付随情報を設けるようにしてもよい。

【００７７】

ディジタル権利管理情報１３２は、コンテンツを使用する規則および状態（Usage rules/status）や、情報サーバ４のウェブページのＵＲＬ（Uniform Resource Locator）等を含んでいる。使用規則および状態としては、例えば、コンテンツの再生回数やコピー回数等が記述される。ＵＲＬは、情報機器１－１が情報サーバ４に対して、ライセンスＩＤ１３３で特定されるライセンスを取得する場合のほか、グループ登録要求、機器登録要求、サービス登録要求機器および登録削除要求を行うときに用いられる情報サーバ４のアドレス情報である。

【００７８】

ライセンスＩＤ１３３は、被暗号化コンテンツ１３６を利用するときに必要とされるライセンスを識別するもので、図５（Ｂ）で説明したものと同じものである。このライセンスＩＤ１３３によって、コンテンツファイル１３０とライセンス１４０とが結びつけられている。

【００７９】

有効化キーブロックＥＫＢ１３４は、後述する階層ツリー構造（図７）の最下層ノードキー（リーフキー）から最上層ノードキー（ルートキーＫＲ）に至る経路のうちの、少なくともルートキーＫＲを含む部分を暗号化してなるものであり、例えば図８（Ａ）に示したような構成を有する。この有効化キーブロックＥＫＢ１３４と、情報サーバ４から付与される鍵情報ＤＮＫとを用いることにより、被暗号化コンテンツ１３６を解読できるようになっている。これについては図７および図８を参照して後述する。

【００８０】

被暗号化コンテンツキー１３５は、有効化キーブロックＥＫＢ１３４から生成されるルートキーＫＲを用いてコンテンツキーＫＣを暗号化したものである。被暗号化コンテンツ１３６は、被暗号化コンテンツキー１３５を解読して得られるコンテンツキーＫＣを用いて暗号化されたものである。

【００８１】

次に、ライセンス１４０について説明する。このライセンス１４０は、ライセ

ンスＩＤ１４１と、作成日時１４２と、有効期限１４３と、使用条件１４４と、リーフＩＤ１４５と、電子署名１４６とを含んでいる。リーフＩＤ１４５を含むことにより、ライセンス１４０はユーザデータ１５０と結びつけられている。なお、ライセンスＩＤ１４１およびリーフＩＤ１４５は、既に説明したものと同義である（図５参照）。

【００８２】

作成日時１４２は、このライセンス１４０を作成した日時である。有効期限１４３は、このライセンス１４０に基づいて、コンテンツを使用することが可能な使用期限である。使用条件１４４には、そのライセンスに基づいてコンテンツをダウンロードすることが可能なダウンロード期限、そのライセンスに基づいてコンテンツをコピーすることが可能な回数（許されるコピー回数）、チェックアウト回数、最大チェックアウト回数、そのライセンスに基づいてコンテンツをＣＤ－ＲＷ等の記録媒体やＰＤ（Portable Device ）等の情報機器に記録することができる権利、ライセンスを所有権（買い取り状態）に移行できる権利、使用ログをとる義務等を示す情報等が含まれる。

【００８３】

次に、ユーザデータ１５０について説明する。ユーザデータ１５０は、機器ＩＤ１５１と、グループＩＤ１５２と、パスワード１５３と、トランザクションＩＤ（ＴＩＤ）１５４と、リーフＩＤ１５５と、鍵情報ＤＮＫ１５６とを含んでいる。リーフＩＤ１５５を含むことにより、ユーザデータ１５０はライセンス１４０に結びつけられている。鍵情報ＤＮＫ１５６を含んでいることにより、これを用いてコンテンツファイル１３０の利用が可能になる。ＴＩＤ１５４は、後述する図９等の各種登録手続きにおいて、各手続き間を相互に結びつけるために用いられるものであり、これにより、ユーザの便宜が図られる。

【００８４】

なお、機器ＩＤ１５１、グループＩＤ１５２、パスワード１５３、リーフＩＤ１５５および鍵情報ＤＮＫ１５６は、図５で説明したものと同義のものである。

【００８５】

図７は、ブロードキャストインクリプション（Broadcast Encryption）方式の

原理に基づいて情報機器（デバイス）およびライセンスキー（コンテンツ解読用の鍵）を管理するために構築される階層ツリー構造Hの一例を表すものである。

【００８６】

この管理方式では、各キーは、ツリー構造における丸印で示したノードにそれぞれ対応して規定される。すなわち、キーは、最上層のルートキーＫＲから最下層のリーフキー（leaf key）まで階層的なツリー構造をなしている。具体的には、最上層のルートノードに対応してルートキーＫＲが規定され、２層目のノードに対応してキーＫ０，Ｋ１が規定され、３層目のノードに対応してキーＫ００～Ｋ１１が規定され、最下層のノードに対応してキーＫ０００～Ｋ１１１が規定されている。例えば、キーＫ０００およびキーＫ００１の上位のキーはＫ００であり、キーＫ００およびキーＫ０１の上位のキーはＫ０であり、キーＫ０およびキーＫ１の上位のキーはルートキーＫＲである。他のキーについても同様であり、いずれのリーフキーからでも、上の階層を遡ればルートキーＫＲに辿り着く構造になっている。上位のキーはその直下のキーによって暗号化されている。

【００８７】

最下層のノードは、ツリー構造における枝葉の位置に当たるのでリーフ（Leaf）と呼ばれ、これに付されるキーＫ０００～Ｋ１１１は、上記したようにリーフキーと呼ばれる。ここに示した例では、各リーフは、番号０から番号７までの８個の機器グループのそれぞれに対応する。各リーフキーは、後述するように（図８参照）、対応するリーフに付与される鍵情報ＤＮＫの一部をなしている。番号０から番号７までの８個の機器グループのそれぞれに対応して、鍵情報ＤＮＫ（ここでは、DNK_0 ～DNK_7）が設定され、さらに、各機器グループの特定識別のために、リーフＩＤ（ここでは、LF_0 ～LF_7）が付与されている。機器グループは、それぞれ、１または２以上のデバイス（情報機器）により構成される。図７に示した例では、機器グループ［０］は３つのデバイス［０］，［１］，［２］により構成され、機器グループ［１］は２つのデバイス［３］，［４］により構成され、機器グループ［２］は４つのデバイス［５］，［６］，［７］，［８］により構成されている。その他の機器グループ［３］～［７］についても同様である。

【００８８】

情報サーバ４から提供されるコンテンツは、階層ツリー構造における最下層のリーフキーから最上層のルートキーＫＲに至る経路上の各ノードキーを用いて多重に暗号化されている。このように多重的に暗号化されたコンテンツを解読して利用可能にするために、例えば図８に示したような構造の有効化キーブロックＥＫＢおよび鍵情報ＤＮＫが用いられる。

【００８９】

図８（Ａ）は、有効化キーブロックＥＫＢの一例を表すものである。ここに示した例では、有効化キーブロックＥＫＢは、Ｅｎｃ（Ｋ０，ＫＲ）およびＥｎｃ（Ｋ１，ＫＲ）という２つのデータにより構成されている。ここで、Ｅｎｃ（Ｋ０，ＫＲ）は、ルートキーＫＲをその直下のノードキーＫ０によって暗号化したデータであり、Ｅｎｃ（Ｋ１，ＫＲ）は、ルートキーＫＲをその直下のノードキーＫ１によって暗号化したデータである。

【００９０】

図８（Ｂ）～（Ｄ）は、鍵情報ＤＮＫの一例を表すものである。（Ｂ）に示したように、機器グループ［0］に付与される鍵情報DNK_0は、Ｅｎｃ（Ｋ００，Ｋ０）、Ｅｎｃ（Ｋ０００，Ｋ００）およびリーフキーＫ０００という３つのデータにより構成されている。Ｅｎｃ（Ｋ００，Ｋ０）は、ノードキーＫ０をその直下のノードキーＫ００によって暗号化したデータであり、Ｅｎｃ（Ｋ０００，Ｋ００）は、ノードキーＫ００をその直下のリーフキーＫ０００によって暗号化したデータである。（Ｃ）に示したように、機器グループ［1］に付与される鍵情報DNK_1は、Ｅｎｃ（Ｋ００，Ｋ０）、Ｅｎｃ（Ｋ００１，Ｋ００）およびリーフキーＫ００１という３つのデータにより構成されている。Ｅｎｃ（Ｋ００，Ｋ０）は、ノードキーＫ０をその直下のノードキーＫ００によって暗号化したデータであり、Ｅｎｃ（Ｋ００１，Ｋ００）は、ノードキーＫ００をその直下のリーフキーＫ００１によって暗号化したデータである。（Ｄ）に示したように、機器グループ［2］に付与される鍵情報DNK_2は、Ｅｎｃ（Ｋ０１，Ｋ０）、Ｅｎｃ（Ｋ０１０，Ｋ０１）およびリーフキーＫ０１０という３つのデータにより構成されている。Ｅｎｃ（Ｋ０１，Ｋ０）は、ノードキーＫ０をその直下の

ノードキーＫ０１によって暗号化したデータであり、Ｅｎｃ（Ｋ０１０，Ｋ０１）は、ノードキーＫ００をその直下のリーフキーＫ０１０によって暗号化したデータである。その他の機器グループ［３］～［７］に付与される鍵情報DNK_3～DNK_7についても同様である（図示せず）。

【００９１】

図７において、例えば、機器グループ［２］に着目すると、この機器グループ［２］に対応するリーフキーＫ０１０からルートキーＫＲに至る経路は、Ｅｎｃ（Ｋ０１０，Ｋ０１），Ｅｎｃ（Ｋ０１，Ｋ０），Ｅｎｃ（Ｋ０，ＫＲ）という３つのデータによって規定される。したがって、図８（Ａ）に示した有効化キーブロックＥＫＢと、図８（Ｃ）に示した鍵情報DNK_2とを組み合わせることにより、階層ツリー構造における最下層から最上層に至る経路上のノードキーを順次解読してルートキーＫＲを取得し、得られたルートキーＫＲを用いてコンテンツを解読することができる。但し、図６に示したように、コンテンツは、ルートキーＫＲによって直接暗号化されているのではなく、ルートキーＫＲによって暗号化された被暗号化コンテンツキーＥｎｃ（ＫＲ，ＫＣ）を用いて暗号化されているので、実際には、ルートキーＫＲによってまず被暗号化コンテンツキーＥｎｃ（ＫＲ，ＫＣ）を解読し、得られたコンテンツキーＫＣを用いて被暗号化コンテンツＥｎｃ（ＫＣ，ＣＯＮＴＥＮＳ）を解読することにより、最終的なコンテンツＣＯＮＴＥＮＳを得ることになる。その他の機器グループについても同様である。

【００９２】

結局、鍵情報DNK_i［ｉ＝０～８］が付与されている機器グループに属する情報機器のみが、暗号を解読してコンテンツを利用できることになる。

【００９３】

このように、本実施の形態では、ユーザが所有する１または２以上のデバイス（情報機器）をまとめて１つの機器グループとし、この機器グループを図７の階層ツリー構造における最下層のリーフノードに割り付けて、リーフＩＤと鍵情報ＤＮＫとを付与するようにしている。その結果、１つの機器グループ内のすべての情報機器に対して同じ（共通の）リーフＩＤおよび鍵情報ＤＮＫが付与される

ことになる。例えば、図７に示した例において、機器グループ［０］の３つのデバイス［０］～［２］には、同じリーフＩＤ（LF_0）および鍵情報DNK_0が付与され、機器グループ［１］の２つのデバイス［３］，［４］には同じリーフＩＤ（LF_1）および鍵情報DNK_1が付与され、機器グループ［２］の４つのデバイス［５］～［８］には、同じリーフＩＤ（LF_2）および鍵情報DNK_2が付与される。その他の機器グループのデバイスについても同様である。

【００９４】

次に、図９～図１２を参照して、以上のような構成の情報処理システムの動作を説明する。なお、図９～図１２は、情報機器１－１，１－２と情報サーバ４との間で行われる一連のやりとりを表すものである。ここでは、情報機器１－１～１－３からなる機器グループ１Ｇを情報サーバ４に登録する場合を例に説明する。なお、以下の説明では、情報機器１－１，１－２は、それぞれ、当初から機器ＩＤ１，ＩＤ２を有するものとして説明する。但し、既に述べたように、機器登録手続きの際に情報機器自身がソフトウェアによって機器ＩＤを生成して保持するようにしてもよい。

【００９５】

まず、図９を参照して、情報機器１－１を用いて機器グループ１Ｇについてのグループ登録を行うと共に、情報機器１－１自身を、その登録した機器グループ１Ｇの一員として登録する場合の処理を説明する。

【００９６】

情報機器１－１ではまず、グループ登録要求機能５２（図３）が、通信機能ブロック７０を介して、情報サーバ４に対してグループ登録要求を行う（図９：ステップＳ２０１）。このグループ登録要求は、情報サーバ４のウェブページにアクセスすることにより行われる。このウェブページにおいて、ユーザが、登録しようとする機器グループに関するグループ情報（ここでは、例えば、ユーザの住所、氏名、電話番号、メールアドレス等のユーザ情報）を入力部２６（図２）から入力し、送信ボタン（図示せず）をクリックすると、このグループ情報がグループ登録要求と共に通信機能ブロック７０を介して情報サーバ４に送信される。

【００９７】

情報サーバ４では、通信機能ブロック１００を介して情報機器１－１からグループ登録要求を受け取ると、グループ登録処理機能９１（図４）が起動して、グループ登録要求からグループ情報を抽出すると共に、グループＩＤおよびパスワードを発行し、これらをグループ情報と共にグループ管理テーブル（図５（Ａ））に登録する。そして、グループ登録処理機能９１は、発行したグループＩＤおよびパスワードをグループ登録完了通知と共に通信機能ブロック１００を介して情報機器１－１に送信する（ステップＳ２０２）。

【００９８】

情報機器１－１では、情報サーバ４から通信機能ブロック７０を介してグループ登録完了通知を受け取ると、グループ登録要求機能５２が、そのグループ登録完了通知からグループＩＤおよびパスワードを抽出し、これらを第３の記憶部８３のユーザデータ１５０（図６）に格納する。

【００９９】

次に、情報機器１－１では、機器登録要求機能５３が、通信機能ブロック７０を介して、情報サーバ４に対して機器登録要求を行う（ステップＳ２０３）。この機器登録要求は、ユーザが情報サーバ４のウェブページにアクセスして、グループＩＤおよびパスワードを入力部２６（図２）から入力し、送信ボタンをクリックすることにより行われる。このとき、機器登録要求機能５３は、ユーザデータ１５０（図６）から機器ＩＤ１を読み出し、この機器ＩＤを、グループＩＤおよびパスワードと共に通信機能ブロック７０を介して情報サーバ４に送信する。

【０１００】

情報サーバ４では、通信機能ブロック１００を介して情報機器１－１から機器登録要求を受け取ると、機器登録管理機能９２（図４）が起動して、機器登録要求から機器ＩＤ１を抽出し、この機器ＩＤ１を、グループＩＤに対応付けてグループ管理テーブル１１３（図５（Ａ））に登録する。このとき、機器登録管理機能９２は、現在の処理（機器登録処理）と次の段階の処理（サーバ登録処理）とを関連付けるためのトランザクションＩＤ１（ＴＩＤ１）を発行し、機器ＩＤ１に対応付けてグループ管理テーブル１１３（図５（Ａ））に登録する。そして、機器登録管理機能９２は、通信機能ブロック１００を介して情報機器１－１に対

し、発行したＴＩＤ１と共に機器登録完了を送信する（ステップＳ２０４）。なお、ＴＩＤ１は、後述するように、それ以降の手続きにおけるユーザの入力負担を軽減するために用いられるものである。なお、後述するように、機器登録可能な最大機器数を越えている場合、機器登録管理機能９２は、その旨を情報機器１－１に送信する。

【０１０１】

情報機器１－１では、情報サーバ４から通信機能ブロック７０を介して機器登録完了通知を受け取ると、機器登録要求機能５３が、その機器登録完了通知からＴＩＤ１を抽出し、このＴＩＤ１を、第３の記憶部８３のユーザデータ１５０（図６）に格納する。

【０１０２】

この段階で、情報サーバ４では、サービス登録処理機能９３が起動し、通信機能ブロック１００を介して、機器登録を完了した情報機器１－１に対してサービス登録（例えば、上記した「ＯｐｅｎＭＧＸ」に基づく登録）を促す通知を行う（ステップＳ２０５）。

【０１０３】

サービス登録を促す通知を受けた情報機器１－１では、サービス登録要求機能５４が起動し、情報サーバ４に対して通信機能ブロック７０を介してサービス登録要求を行う（ステップＳ２０６）。このサービス登録要求は、例えば、情報サーバ４から送られてきたサービス登録用のウェブページにおいて、ユーザが同意ボタン（図示せず）をクリックすることにより行われる。すなわち、ユーザのクリック操作に応じ、サービス登録要求機能５４は、ユーザデータ１５０（図６）からＴＩＤ１を読み出し、サービス登録要求と共に情報サーバ４に送信する。したがって、ユーザは、更めてグループＩＤおよびパスワードを入力する必要はない。

【０１０４】

情報サーバ４では、通信機能ブロック１００を介して情報機器１－１からサービス登録要求を受け取ると、サービス登録処理機能９３（図４）が起動して、サービス登録要求からＴＩＤ１を抽出し、抽出したＴＩＤ１を基に、どの情報機器

からのサービス登録要求であるか、および、このサービス登録要求をしてきた情報機器を所有するユーザがサービス登録を済ましてあるか否かを判断する。ここでは、グループ登録の済んでいない機器グループに属する情報機器１－１からの要求であると判断し、リーフＩＤと鍵情報ＤＮＫとを発行すると共に、これらを、情報機器１－１のグループＩＤに対応付けてグループ管理テーブル１１３（図５（Ａ））に登録する。そして、サービス登録処理機能９３は、情報機器１－１に対して、リーフＩＤと鍵情報ＤＮＫとを含むサービスデータを、サービス登録完了通知と共に通信機能ブロック１００を介して送信する（ステップＳ２０７）。

【０１０５】

情報機器１－１では、通信機能ブロック７０を介して情報サーバ４からサービス登録完了通知を受け取ると、サービス登録要求機能５４が、そのサービス登録完了通知から、リーフＩＤおよび鍵情報ＤＮＫを含むサービスデータを抽出し、このサービスデータを、グループＩＤと共に第３の記憶部８３のユーザデータ１５０（図６）にセキュアに（安全かつ秘密裏に）保存する。この段階で、情報機器１－１にとってコンテンツの利用に必要なすべての事前登録が完了する。したがって、これ以降、ユーザは、情報機器１－１を介して情報サーバ４にアクセスしてコンテンツおよびライセンスをダウンロードし、そのダウンロードしたコンテンツを利用したり、あるいは、機器グループ１Ｇ内の他の情報機器１－２等によりダウンロードして取得したコンテンツおよびライセンスを情報機器１－１にコピーして利用することが可能となる。その詳細は後述する。

【０１０６】

次に、図１０を参照して、情報機器１－２を機器グループ１Ｇの一員に加える場合の処理を説明する。この処理は、基本的に、情報機器１－１を機器グループ１Ｇの一員に加える場合の処理（ステップＳ２０３～Ｓ２０７）とほぼ同様であるので、同様の記載は適宜省略する。

【０１０７】

まず、情報機器１－２では、機器登録要求機能５３が、通信機能ブロック７０を介して情報サーバ４に対して機器登録要求を行う（図１０：ステップＳ２０８

）。この機器登録要求は、ユーザが情報サーバ４のウェブページにアクセスして、情報機器１－１によって既に取得済のグループＩＤおよびパスワードを入力部２６（図２）から入力し、送信ボタンをクリックすることにより行う。これにより、機器登録要求機能５３は、ユーザデータ１５０（図６）から機器ＩＤ２を読み出し、この機器ＩＤ２を、ユーザが入力したグループＩＤおよびパスワードと共に情報サーバ４に送信する。このとき、機器登録要求機能５３は、入力されたグループＩＤおよびパスワードを、機器ＩＤ２と共に第３の記憶部８３（図３）のユーザデータ１５０（図６）に格納する。

【０１０８】

情報サーバ４では、通信機能ブロック１００を介して情報機器１－２から機器登録要求を受け取ると、機器登録管理機能９２が、機器登録要求から機器ＩＤ２を抽出し、この機器ＩＤ２を、グループＩＤに対応付けてグループ管理テーブル１１３（図５（Ａ））に追加登録する。機器登録管理機能９２はまた、トランザクションＩＤ２（ＴＩＤ２）を発行し、機器ＩＤ２に対応付けてグループ管理テーブル１１３に記憶する。そして、機器登録管理機能９２は、情報機器１－２に対し、発行したＴＩＤ２と共に通信機能ブロック１００を介して機器登録完了を送信する（ステップＳ２０９）。なお、ＴＩＤ２は、上記のＴＩＤ１と同様の目的で用いられるものである。

【０１０９】

情報機器１－２では、通信機能ブロック７０を介して情報サーバ４から機器登録完了通知を受け取ると、機器登録要求機能５３が、その機器登録完了通知からＴＩＤ２を抽出し、このＴＩＤ２を、第３の記憶部８３のユーザデータ１５０（図６）に格納する。

【０１１０】

この段階で、情報サーバ４では、サービス登録処理機能９３が起動し、通信機能ブロック１００を介して、機器登録を完了した情報機器１－２に対して、サービス登録を促す通知を行う（ステップＳ２１０）。この通知は、例えばサービス登録用のウェブページを情報機器１－２に送信することで行う。

【０１１１】

サービス登録を促す通知を受けた情報機器１－２では、サービス登録要求機能５４が起動して、通信機能ブロック７０を介して、情報サーバ４に対するサービス登録要求を行う（ステップＳ２１１）。このサービス登録要求は、上記の情報機器１－１の場合と同様に、情報サーバ４から送られてきたサービス登録用のウェブページにおいて、ユーザが同意ボタン（図示せず）をクリックすることにより行われる。すなわち、ユーザのクリック操作に応じ、サービス登録要求機能５４は、第３の記憶部８３のユーザデータ１５０（図６）からＴＩＤ２を読み出し、これを、サービス登録要求と共に情報サーバ４に送信する。したがって、ユーザは、更めてグループＩＤおよびパスワードを入力する必要はない。

【０１１２】

情報サーバ４では、通信機能ブロック１００を介して情報機器１－２からサービス登録要求を受け取ると、サービス登録処理機能９３（図４）が起動して、サービス登録要求からＴＩＤ２を抽出し、抽出したＴＩＤ２を基に、どの情報機器からのサービス登録要求であるか、および、グループ登録が済んでいるか否かを判断する。ここでは、グループ登録済の機器グループ１Ｇに属する情報機器１－２からの要求であると判断し、グループ管理テーブル１１３から、情報機器１－２のグループＩＤに対応して登録されているリーフＩＤと鍵情報ＤＮＫとを読み出し、これらを含むサービスデータを、サービス登録完了通知と共に通信機能ブロック１００を介して送信する（ステップＳ２１２）。

【０１１３】

情報機器１－２では、通信機能ブロック７０を介して情報サーバ４からサービス登録完了通知を受け取ると、サービス登録要求機能５４が、このサービス登録完了通知からリーフＩＤおよび鍵情報ＤＮＫを抽出し、これらの抽出情報を、第３の記憶部８３のユーザデータ１５０（図６）に登録する。この段階で、情報機器１－２にとってコンテンツの利用に必要なすべての事前登録が完了する。したがって、これ以降、ユーザは、情報機器１－２を介して情報サーバ４にアクセスしてコンテンツおよびライセンスをダウンロードし、そのダウンロードしたコンテンツを利用したり、あるいは、機器グループ１Ｇ内の他の情報機器１－１等によりダウンロードして取得したコンテンツおよびライセンスを情報機器１－２に

コピーして利用することが可能となる。その詳細は後述する。

【０１１４】

以下、同様にして、機器グループ１Ｇ内の他の情報機器１－３についても、機器登録処理とサービス登録処理とを行うことにより、ユーザは、情報機器１－３を介して情報サーバ４にアクセスしてコンテンツおよびライセンスをダウンロードし、そのダウンロードしたコンテンツを利用したり、あるいは、機器グループ１Ｇ内の他の情報機器１－１等によりダウンロードして取得したコンテンツおよびライセンスを情報機器１－３にコピーして利用することが可能となる。

【０１１５】

なお、本実施の形態では、トランザクションＩＤを利用して、機器登録手続きとさらに登録手続きとを関連付けるようにしたが、これは必ずしも必要ではなく、省略可能である。この場合には、サービス登録要求の際に（ステップＳ２０６）、ユーザに対してグループＩＤおよびパスワードの入力を求めるようにすればよい。

【０１１６】

このようにして、情報サーバ４は、ユーザが所有する複数の情報機器を束ねて１つの機器グループとして認識するようになるが、この機器登録を無制限に認めると、実質上、コンテンツの利用に制限がなくなり、ライセンサーの不利益が大きくなる。この弊害を回避するため、本実施の形態では、上記のように、１つの機器グループに含めることができる情報機器の数に制限を設けている。具体的には、情報サーバ４は、いずれかの情報機器から機器登録要求があった場合に、グループ管理テーブル１１３（図５（Ａ））の１つの機器グループに登録されている機器ＩＤの数をチェックし、この数が所定数ｎに達したときは、それ以降、機器登録要求を拒否し、その旨を情報機器に通知する。なお、通常、１人のユーザが登録できる情報機器の最大数は、配信サービスを行う事業者の運用ルールで決定される。

【０１１７】

また、例えば、ユーザが登録した情報機器の数が登録可能数の上限ｎまで達したのち、例えば、ユーザが所有する情報機器を買い換えた場合のように、他の新

たな情報機器を登録したい場合には、一旦、機器登録削除を行って登録機器の数を減らし、その後更めて、登録したい情報機器についての登録要求を行うようにすればよい。以下、この登録削除の手続きを図１１を参照して説明する。ここでは、既に機器登録がなされている情報機器１－２についての登録削除を行う場合について説明する。

【０１１８】

この場合、まず、情報機器１－２では、機器登録削除要求機能５５が、情報サーバ４に対して機器登録削除要求を行う（図１１：ステップＳ２１３）。この機器登録削除要求は、ユーザが情報サーバ４のウェブページにアクセスして、既に取得済のグループＩＤおよびパスワードを入力し、送信ボタンをクリックすることにより行う。このとき、機器登録削除要求機能５５は、ユーザデータ１５０から機器ＩＤ２を読み出し、この機器ＩＤ２を、ユーザが入力したグループＩＤおよびパスワードと共に情報サーバ４に送信する。

【０１１９】

情報サーバ４では、情報機器１－２から機器登録削除要求を受け取ると、機器登録管理機能９２が、機器登録要求から機器ＩＤ２を抽出し、この機器ＩＤ２を、グループ管理テーブル１１３から削除する。そして、機器登録管理機能９２は、情報機器１－２に対し、機器登録削除完了通知を送信する（ステップＳ２１４）。

【０１２０】

情報機器１－２では、情報サーバ４から機器登録削除完了通知を受け取ると、機器登録削除要求機能５５が、第３の記憶部８３のユーザデータ１５０から、リーフＩＤおよび鍵情報ＤＮＫを含むサービスデータを削除する。この結果、例えば図１１の例では、グループ管理テーブル１１３に登録された機器ＩＤは、情報機器１－１についての機器ＩＤ１のみとなり、情報機器１－２は機器グループ１Ｇから外される。したがって、それ以降は、該当するコンテンツを情報機器１－２で利用することはできなくなる。

【０１２１】

次に、図１２を参照して、コンテンツおよびライセンスの提供・取得処理につ

いて説明する。なお、コンテンツは情報サーバ４の側に予め作り置きされており、グループ登録、機器登録およびサービス登録を済ましていない者やライセンスを取得していない者であっても、コンテンツ自体をダウンロードをすることはできるが、後述するように、それらの登録やライセンス取得をしていなければ、コンテンツの利用はできない。

【０１２２】

コンテンツのダウンロードを行う場合、情報機器１－１では、まず、ユーザの入力操作に応じて、コンテンツ・ライセンス要求機能５７が起動し、通信機能ブロック７０を介して、情報サーバ４に対して、コンテンツ要求を行う（図１２：ステップＳ２１５）。具体的には、ユーザが入力部２６を操作して、提供を受けようとするコンテンツを指定すると、コンテンツ・ライセンス要求機能５７は、このコンテンツを指定する情報（コンテンツ指定情報）を取り込み、このコンテンツ指定情報を、コンテンツ要求と共に情報サーバ４に送信する。

【０１２３】

情報サーバ４では、情報機器１－１から通信機能ブロック１００を介してコンテンツ要求を受け取ると、コンテンツ・ライセンス提供機能９４が起動し、受け取ったコンテンツ要求からコンテンツ指定情報とを抽出する。コンテンツ・ライセンス提供機能９４はさらに、コンテンツ蓄積部１１１から、その抽出したコンテンツ指定情報が指すコンテンツファイルを読み出し、その読み出したコンテンツファイルを、通信機能ブロック１００を介して情報機器１－１に送信する（ステップＳ２１６）。

【０１２４】

情報機器１－１では、情報サーバ４から通信機能ブロック７０を介してコンテンツファイルを受け取ると、コンテンツ・ライセンス要求機能５７が、そのコンテンツファイルを第１の記憶部８１に格納する。これにより、情報機器１－１は、図６に示したように、ライセンスＩＤによってライセンス１４０にリンクされたコンテンツファイル１３０を保有することとなる。

【０１２５】

次に、ライセンスの取得手順について説明する。ここではまず、情報機器１－

１を用いて情報サーバ４にアクセスしてライセンスを購入する場合について説明する。

【０１２６】

ライセンスを取得する場合、情報機器１－１では、まず、ユーザの入力操作に応じて、コンテンツ・ライセンス要求機能５７が起動し、通信機能ブロック７０を介して、情報サーバ４に対して、ライセンス要求を行う（図１２：ステップＳ２１７）。具体的には、ユーザが入力部２６を操作して、既に取得してあるグループＩＤとパスワードとを入力し、上記でダウンロードしたコンテンツを利用するのに必要なライセンスを指定すると、コンテンツ・ライセンス要求機能５７は、そのライセンスを指定する情報（ライセンス指定情報）を取り込むと共に、ユーザデータ１５０（図6）からリーフＩＤを読み出し、このリーフＩＤおよびライセンス指定情報を、ライセンス要求と共に情報サーバ４に送信する。

【０１２７】

情報サーバ４では、情報機器１－１から通信機能ブロック１００を介してライセンス要求を受け取ると、コンテンツ・ライセンス提供機能９４が起動し、受け取ったライセンス要求からリーフＩＤとライセンス指定情報とを抽出する。コンテンツ・ライセンス提供機能９４はさらに、ライセンステーブル１１２（図５（Ｂ））から、その抽出したライセンス指定情報に対応するライセンスＩＤおよびライセンスの内容を読み出し、これらに、ライセンス要求から抽出したリーフＩＤを付加する。ライセンスの内容には、バージョン、作成日時、有効期限および使用条件等の情報が含まれている。さらに、秘密鍵（図示せず）を用いて署名を付加することにより、図6に示したようなフォーマット形式のライセンス１４０を作成し、情報機器１－１に送信する（ステップＳ２１８）。このとき、コンテンツ・ライセンス提供機能９４は、そのリーフＩＤに対応するグループＩＤ（この場合、情報機器１－１が属する機器グループ１Ｇのグループ ＩＤ）を、グループ管理テーブル１１３（図５（Ａ））から読み出し、このグループＩＤが、ライセンステーブル１１２中の該当する（提供しようとする）ライセンスＩＤに対応付けて登録されているか、否かを判断する。その結果、そのグループＩＤが登録されていない場合には、そのライセンスが未だ情報機器１－１によって購入され

ていないと判断し、そのグループＩＤを、ライセンステーブル１１２中の該当する（提供しようとする）ライセンスＩＤに対応付けて登録すると共に、課金処理機能９５（図４）が課金処理を実行する。一方、そのグループＩＤが登録されている場合には、課金処理を行わない。ここで示した例では、対象としているライセンスの取得は、情報機器１－１が属する機器グループ１Ｇにおいて初めて行うものなので、ライセンスの購入と判断され、課金処理が行われる。

【０１２８】

情報機器１－１では、情報サーバ４から通信機能ブロック７０を介してライセンスを受け取ると、コンテンツ・ライセンス要求機能５７が、そのコンテンツファイルを第２の記憶部８２に格納する。これにより、情報機器１－１は、図６に示したように、リーフＩＤによってユーザデータ１５０とリンクされたライセンス１４０を保有することとなる。したがって、これ以降、ユーザは、そのライセンスの示す条件の範囲内において、情報機器１－１を用いて、そのコンテンツを自由に利用することができる。

【０１２９】

なお、ライセンス取得処理は、コンテンツを取得する前に予め行っておくようにすることも可能である。

【０１３０】

次に、情報機器１－２から情報サーバ４にアクセスして、既に情報機器１－１が取得したものと同じライセンスを取得する場合について説明する。

【０１３１】

この場合のライセンス取得処理は、基本的には、上記の情報機器１－１による処理と同様である。但し、この場合、機器グループ１Ｇ内でのライセンス取得は情報機器１－１に続いて２度目であるので、この点に関して、情報サーバ４は異なる処理を行う。すなわち、コンテンツ・ライセンス提供機能９４は、情報機器１－２からのライセンス要求から抽出したリーフＩＤに対応するグループＩＤ（ここでは、情報機器１－２が属する機器グループ１ＧのグループＩＤ）を、グループ管理テーブル１１３（図５（Ａ））から読み出し、このグループＩＤが、ライセンステーブル１１２中の該当する（提供しようとする）ライセンスＩＤに

対応付けて登録されているか、否かを判断する。ここでは、そのグループＩＤがライセンステーブル１１２に既に登録されているので、情報サーバ４の課金処理機能９５（図４）は、課金処理を行わない。その他の処理は、情報機器１－１によるライセンス取得（購入）の場合と同様である。

【０１３２】

このように、ユーザは、情報機器１－１を用いて情報サーバ４から購入したライセンスと同一のライセンスを、機器グループ１Ｇ内の他の情報機器１－２を用いて、更めて料金を支払うことなく、情報サーバ４から再取得することが可能となる。このようなライセンスの再取得は、機器グループ１Ｇ内の別の情報機器１－３からも同様に行うことができ、料金はかからない。

【０１３３】

次に、図１３を参照して、情報機器１－１を用いてコンテンツを再生する場合の処理について説明する。

【０１３４】

ユーザが入力部２６を操作してコンテンツの再生を指示すると、再生処理機能５１（図３）が起動し、その指定されたコンテンツに対応するライセンスＩＤ１３３を、第１の記憶部８１に格納されているコンテンツファイル１３０（図６）から読み取る。再生処理機能５１は、読み取ったライセンスＩＤ１３３に対応するライセンスが取得されているか否かを判定する。ライセンスが既に取得されていると判定された場合、再生処理機能５１は、その取得されているライセンスが有効期限内のものであるか否かを判定する。なお、ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている有効期限１４３（図６）と、タイマ２０により計時されている現在日時とを比較することで判断される。ライセンスの有効期限が既に満了していると判定された場合には、ユーザにたいし、ライセンス更新処理の実行等を促す。

【０１３５】

次に、再生処理機能５１は、読み取ったライセンスＩＤ１３３を基に、第２の記憶部８２に格納されているライセンス１４０（図６）からリーフＩＤ１４５を読み取る。さらに、再生処理機能５１は、読み取ったリーフＩＤを基に、第３の

記憶部８３のユーザデータ１５０（図６）から鍵情報ＤＮＫ１５６を読み取る。再生処理機能５１は、この鍵情報ＤＮＫ１５６を用いて、コンテンツファイル１３０（図６）の有効化キーブロックＥＫＢ１３４を解読して、ルートキーＫＲを得る。例えば、情報機器１－１が機器グループ［０］に属するものであるとすると、鍵情報$ＤＮＫ_0$（図８（Ｂ）参照）を用いて有効化キーブロックＥＫＢ（図８（Ａ））を解読する。具体的には、まず、鍵情報$ＤＮＫ_0$の中のリーフキーＫ０００を用いてＥｎｃ（Ｋ０００，Ｋ００）を解読してノードキーＫ００を取得し、これにより得られたノードキーＫ００を用いてＥｎｃ（Ｋ００，Ｋ０）を解読してノードキーＫ０を取得し、これにより得られたノードキーＫ０を用いて有効化キーブロックＥＫＢのＥｎｃ（Ｋ０，ＫＲ）を解読してルートキーＫＲを取得する。再生処理機能５１は、こうして得られたルートキーＫＲを用いて、被暗号化コンテンツキー１３５（＝Ｅｎｃ（ＫＲ，ＫＣ））を解読して、コンテンツキーＫＣを取得し、得られたコンテンツキーＫＣを用いて被暗号化コンテンツ１３６（＝Ｅｎｃ（ＫＣ，ＣＯＮＴＥＮＴＳ））を解読し、最終的に、利用可能な態様のコンテンツＣＯＮＴＥＮＳを得る。再生処理機能５１は、こうして解読したコンテンツを再生し、出力部２７から出力する。

【０１３６】

情報機器１－２，１－３を用いてコンテンツを再生する場合の処理も同様である。

【０１３７】

なお、情報機器１－２，１－３に関しては、コンテンツおよびライセンスの取得方法が２通りある。第１の方法は、上記したように、情報サーバ４から直接ダウンロードする方法である。第２の方法は、情報機器１－１によって情報サーバ４からダウンロードしたコンテンツおよびライセンスを、そっくり情報機器１－２にコピーする方法である。これらのいずれの方法においても、情報機器１－２，１－３は、取得したコンテンツを解読して再生することができる。なぜなら、これらの情報機器１－２，１－３は、情報サーバ４に対する機器登録およびサービス登録をそれぞれ行ったことにより、コンテンツの再生に必要なサービスデータ（リーフＩＤと鍵情報ＤＮＫとを含む）を既に取得し、保持しているからであ

る。

【０１３８】

以上のように、本実施の形態によれば、情報サーバにおいてユーザ（機器グループ）とその機器グループ内の各情報機器とを関連付けて管理し、同一ユーザの所有する情報機器には、同一のサービスデータ（リーフＩＤおよび鍵情報ＤＮＫ）を書き込むことにより、ユーザの所有する複数の情報機器を１つのグループとして扱うようにしたので、同一グループ内の情報機器間では、同一のコンテンツおよびライセンスを利用することが可能となる。具体的には、例えば、ある情報機器のコンテンツおよびライセンスを、通常のファイルを操作する方法により、同一グループ内の別の情報機器にコピーすれば、その機器においてもコンテンツの再生が可能になる。すなわち、ユーザは、一旦、ある情報機器でコンテンツおよびライセンスをダウンロードしておけば、自己の所有する情報機器間に関する限り、通常のコピーを行うだけで、他の情報機器でコンテンツを利用することが可能になる。このため、それぞれの情報機器を何度もネットワークを介してサーバに接続してダウンロードする必要がなくなる。

【０１３９】

また、ある情報機器により情報サーバからコンテンツおよびライセンスを入手し、その後、同一グループ内の異なる情報機器によって、再び情報サーバから、その同じコンテンツおよびライセンスを入手することも可能である。その際には、課金処理は発生しない。これにより、例えばユーザが、利用したいコンテンツが保存されている自己の情報機器から遠く離れた場所にいる場合であっても、その時点で所有している他の情報機器によってコンテンツを利用することも可能となる。

【０１４０】

以上をまとめると、次のことが言える。

【０１４１】

（１）コンテンツを正当な方法で入手したユーザのみが再生可能となるように保護されたコンテンツを配信するシステムにおいて、ユーザがある情報機器で取得したコンテンツを、ユーザが所有する他の情報機器でも利用することが可能とな

る。

（2）ネットワークを介してサーバに接続するという方法ではなく、情報機器間で直接コンテンツやライセンスの移動が可能となる。

（3）コンテンツを入手した情報機器と同じグループに属する他の情報機器を用いて、ネットワークを経由して情報サーバから課金処理の発生なしにコンテンツおよびライセンスを入手することができる。

（4）ユーザが所有する情報機器を買い換えた場合においても、その新たな情報機器を用いて、入手済のコンテンツを利用することが可能となる。

【0142】

以上、実施の形態を挙げて本発明を説明したが、本発明はこの実施の形態に限定されず、種々の変形が可能である。例えば、上記実施の形態では、1つの情報サーバ4によって各種の登録処理等を行うようにしたが、コンテンツ提供処理、ライセンス提供処理、サービス登録処理および課金処理を互いに別の（物理機械的に独立した）サーバによって行うようにしてもよい。

【0143】

また、本実施の形態では、情報機器は情報サーバとの間でオンラインで各種の登録手続きやダウンロードを行うものとして説明したが、本発明はこれに限定されず、オフラインで登録手続き等を行うようにしてもよい。この場合には、例えば、コンテンツ、ライセンスおよび各種登録手続き用プログラムを、CD－R等のような可搬性の追記型記録媒体に収納して事業者がユーザに配布し、ユーザは、そのプログラムを自己の情報機器にインストールして実行させることにより、各種登録手続きと、コンテンツおよびライセンスの取得とを実現することができる。したがって、インターネット等の通信回線に接続し得る環境にない情報機器を有するユーザにも対応することができる。

【0144】

また、本実施の形態では、1のユーザは1の機器グループを登録できるものとして説明したが、1のユーザが複数の機器グループを登録できるようにしてもよい。なお、1のユーザは、一般的には一個人を指すが、必ずしもこれに限定されず、ライセンサーが許容するのであれば、例えば、生計を共にする1つの家族全

体や１つの社会的組織が１のユーザとなることができるようにしてもよい。さらには、１のユーザの内部を階層化して管理するようにしてもよい。例えば、１つの企業を１つのユーザとし、その企業内の複数の事業部をそれぞれサブユーザとする場合が該当する。この場合には、コンテンツやライセンスの種類や内容、性質、あるいは配布形態等に応じて、多様な管理態様や利用態様が想定され、実益があると考えられる。

【０１４５】

また、情報機器としては、様々な機器が想定される。例えば、電子書籍機器や電子辞書等の専用機器のほか、例えば、パーソナルコンピュータ等の汎用のコンピュータや、携帯電話等の汎用のＰＤ機器にも適用可能である。専用機器としては、上記のほかに、例えば、ＣＤやＭＤ（商標）、あるいはＩＣプレーヤ等のオーディオ再生機器、ＤＶＤに代表されるビデオ再生機器、さらには、ＨＤ内蔵のテレビジョン受像機やゲーム機等も含まれる。

【０１４６】

【発明の効果】

以上説明したように、本発明の情報機器または第１の情報処理プログラムによれば、コンテンツとライセンスとを記憶すると共に、グループ化機器識別情報とコンテンツ解読用の鍵情報とグループ識別子とを保有しておき、ライセンスに含まれる情報と、グループ化機器識別情報と、コンテンツ解読用の鍵情報と、グループ識別子とをリンクさせた処理を行うことによりコンテンツを解読するようにしたので、同じグループ化機器識別情報および鍵情報をもつ情報機器であれば、コンテンツを自由に利用可能になる。

【０１４７】

本発明の情報サーバまたは第２の情報処理プログラムによれば、情報機器からのグループ登録要求に応じて、登録対象の機器グループに関する情報をグループ識別子に対応付けて登録すると共に、情報機器からのサービス登録要求に応じて、登録を要求してきた情報機器をサービス提供対象として登録し、一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録すると共に、登録を要求してきた情報機器が属する機器グループ内のすべ

ての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するようにしたので、その機器グループ内のすべての情報機器が、同じグループ化機器識別情報および鍵情報をもつことになる。このため、機器グループ内のすべての情報機器においてコンテンツを自由に利用可能になる。すなわち、ユーザがある情報機器で取得したコンテンツを、ユーザが所有する他の情報機器でも利用することも可能となる。また、ネットワークを介してサーバに接続するという方法によるのではなく、情報機器間で直接コンテンツやライセンスを移動するという方法により、情報機器間でのコンテンツ利用が可能になる。

【０１４８】

特に、一旦登録された機器識別情報を情報サーバから削除することを情報機器が要求し、これに応じて、情報サーバがその登録削除を行うようにした場合には、ユーザが現に使用している情報機器を他の新たな情報機器に取り替えることも可能になる。

【０１４９】

また、情報機器が機器識別情報生成機能を備えるようにした場合には、機器識別情報が付与されていない既存の情報機器であっても、あとから機器識別情報を付与することができ、本発明が適用可能になる。

【０１５０】

また、一の機器グループについて登録された機器識別情報の数が一定数に達した以降は、情報サーバがその機器グループに属する新たな情報機器からの機器登録要求を拒否するようにした場合には、１つの機器グループに登録される情報機器の数が無制限に増えるのを防ぐことができる。

【０１５１】

また、ライセンス要求に応じてライセンスを情報機器に提供する際に、そのライセンス要求からグループ化機器識別情報を抽出すると共に、その抽出されたグループ化機器識別情報に基づいて、そのライセンスが、そのライセンス要求をしてきた情報機器の属する機器グループによって既に購入されたものであるか否かを調べ、その結果に応じて、ライセンス提供に伴う課金処理を行うか否かを判定するようにした場合には、機器グループ内の情報機器を用いてライセンスを一旦

購入しておけば、その機器グループ内の情報機器からライセンスを再取得する場合に、ライセンス料の再度の支払いを免れることができる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態に係る情報処理システムの全体構成を表すブロック図である。

【図２】

情報機器および情報サーバの要部構成を表すブロック図である。

【図３】

情報機器の機能構成の要部を表すブロック図である。

【図４】

情報サーバの機能構成の要部を表すブロック図である。

【図５】

情報サーバにおけるグループ管理テーブルおよびライセンステーブルの一例を表す図である。

【図６】

情報機器におけるコンテンツファイル、ライセンスおよびユーザデータの内容の一例を表す図である。

【図７】

情報サーバによって管理される暗号解読キーにおける階層ツリー構造の一例を表す図である。

【図８】

図８の階層ツリー構造に適用される有効化キーブロックおよび鍵情報の内容の一例を表す図である。

【図９】

情報機器と情報サーバとの間で行われるグループ登録処理、機器登録処理およびサービス登録処理を説明するための図である。

【図１０】

情報機器と情報サーバとの間で行われる機器登録処理およびサービス登録処理

を説明するための図である。

【図１１】

情報機器と情報サーバとの間で行われる機器登録削除処理を説明するための図である。

【図１２】

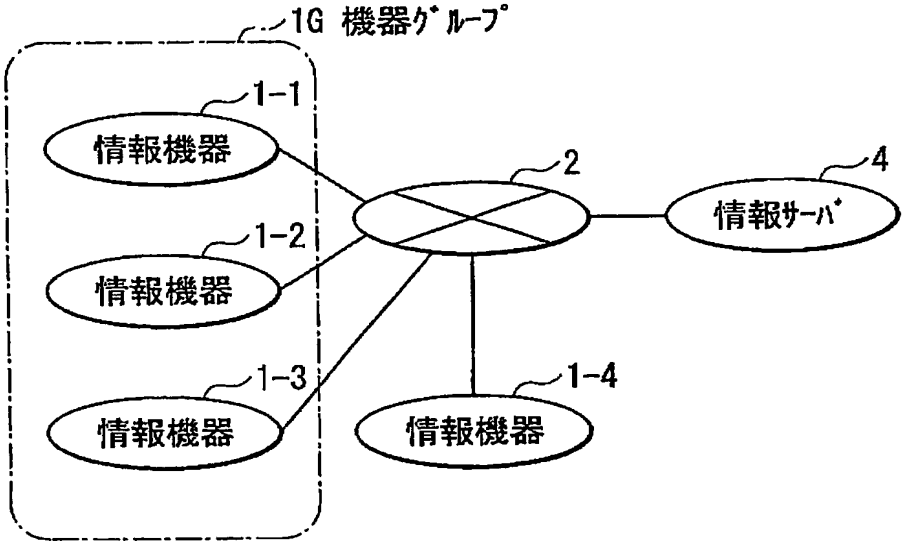
情報機器と情報サーバとの間で行われるコンテンツおよびライセンスのダウンロード処理を説明するための図である。

【符号の説明】

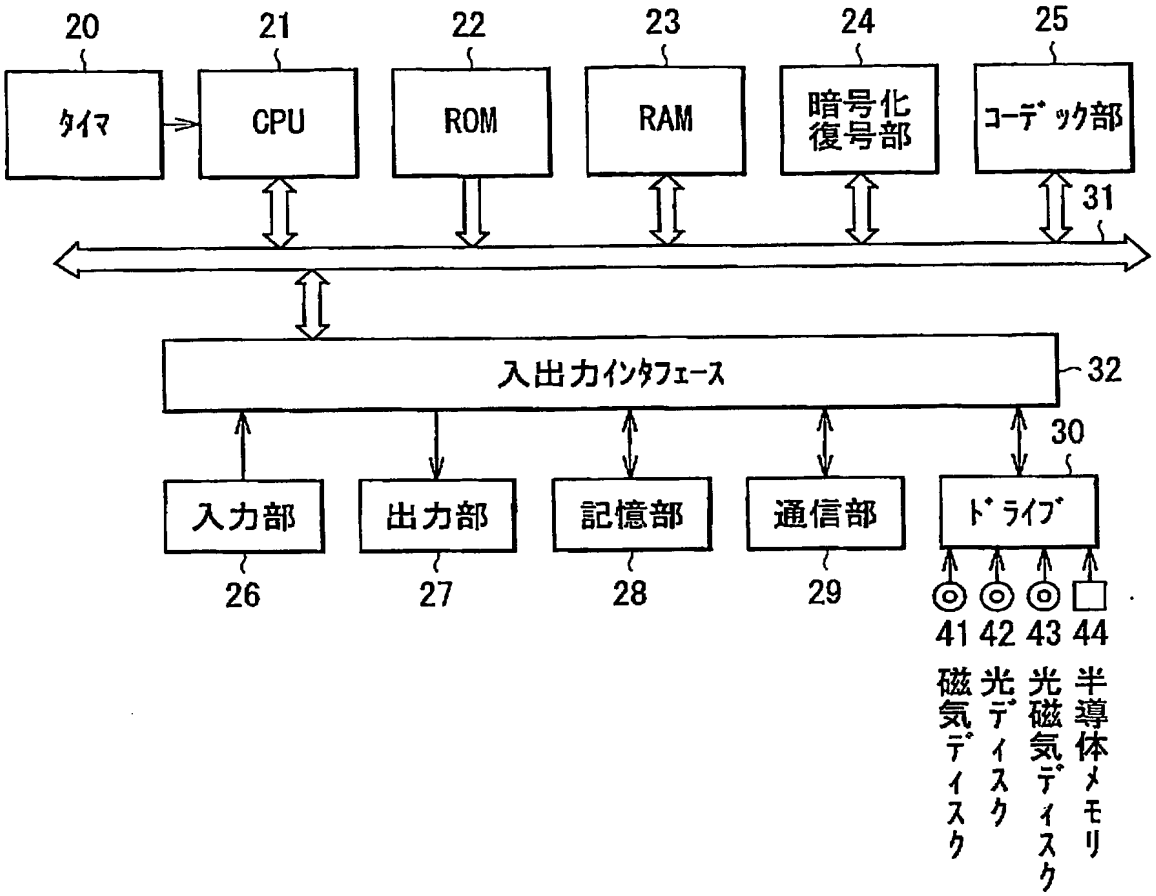
１－１～１－４…情報機器、１Ｇ…機器グループ、２…インターネット、４…情報サーバ、２１…ＣＰＵ、２２…ＲＯＭ、２４…暗号化復号部、２６…入力部、２７…出力部、２８…記憶部、２９…通信部、５０，９０…制御機能ブロック、５１…再生処理機能、５２…グループ登録要求機能、５３…機器登録要求機能、５４…サービス登録要求機能、５５…コンテンツ・ライセンス提供機能、７０，１００…通信機能ブロック、８０，１１０…記憶機能ブロック、８１…第１の記憶部、８２…第２の記憶部、８３…第３の記憶部、８４…第４の記憶部、９１…グループ登録処理機能、９２…機器登録管理機能、９３…サービス登録処理機能、９４…コンテンツ・ライセンス提供機能、９５…課金処理機能、１１１…コンテンツ蓄積機能、１１２…ライセンステーブル、１１３…グループ管理テーブル、１２２…パスワード、１２３…グループ情報、１２４…機器ＩＤ、１２５…サービスデータ、１２７、１３３，１４１…ライセンスＩＤ、１３０…コンテンツファイル、１３１…コンテンツＩＤ、１３４…有効化キーブロックＥＫＢ、１４０…ライセンス、１４５，１５５…リーフＩＤ、１５０…ユーザデータテーブル、１５２…グループＩＤ、１５６…鍵情報ＤＮＫ。

【書類名】　図面

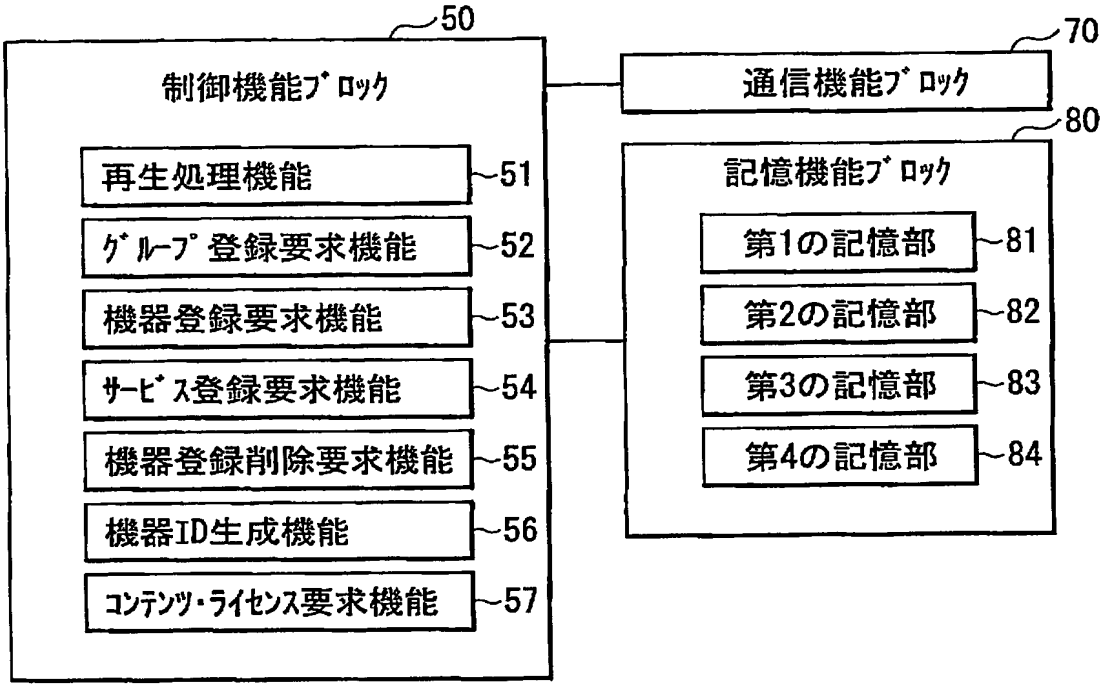
【図１】



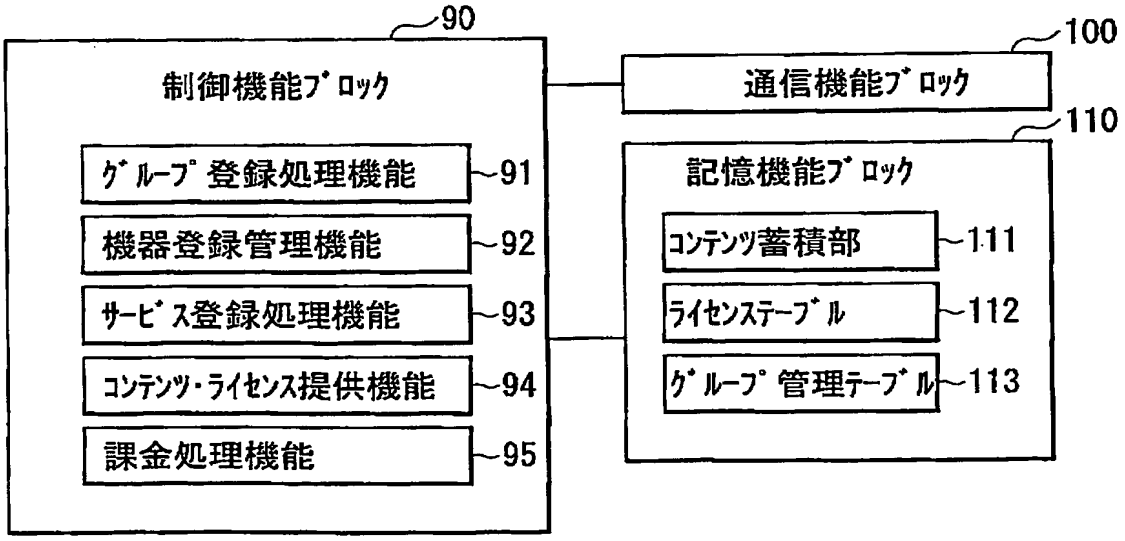
【図２】


20
21
22
23
24
25
タイマ
CPU
ROM
RAM
暗号化
復号部
コーデック部
31
入出力インタフェース
32
30
入力部
出力部
記憶部
通信部
ドライブ
26
27
28
29
41
42
43
44
磁気ディスク
光ディスク
光磁気ディスク
半導体メモリ

【図３】


50
制御機能ﾌﾞﾛｯｸ
再生処理機能
51
ｸﾞﾙｰﾌﾟ登録要求機能
52
機器登録要求機能
53
ｻｰﾋﾞｽ登録要求機能
54
機器登録削除要求機能
55
機器ID生成機能
56
ｺﾝﾃﾝﾂ・ﾗｲｾﾝｽ要求機能
57
70
通信機能ﾌﾞﾛｯｸ
80
記憶機能ﾌﾞﾛｯｸ
第1の記憶部
81
第2の記憶部
82
第3の記憶部
83
第4の記憶部
84

【図４】


90
制御機能ﾌﾞﾛｯｸ
ｸﾞﾙｰﾌﾟ登録処理機能
91
機器登録管理機能
92
ｻｰﾋﾞｽ登録処理機能
93
ｺﾝﾃﾝﾂ・ﾗｲｾﾝｽ提供機能
94
課金処理機能
95
100
通信機能ﾌﾞﾛｯｸ
110
記憶機能ﾌﾞﾛｯｸ
ｺﾝﾃﾝﾂ蓄積部
111
ﾗｲｾﾝｽﾃｰﾌﾞﾙ
112
ｸﾞﾙｰﾌﾟ管理ﾃｰﾌﾞﾙ
113

【図５】

(A)

113 グループ管理テーブル

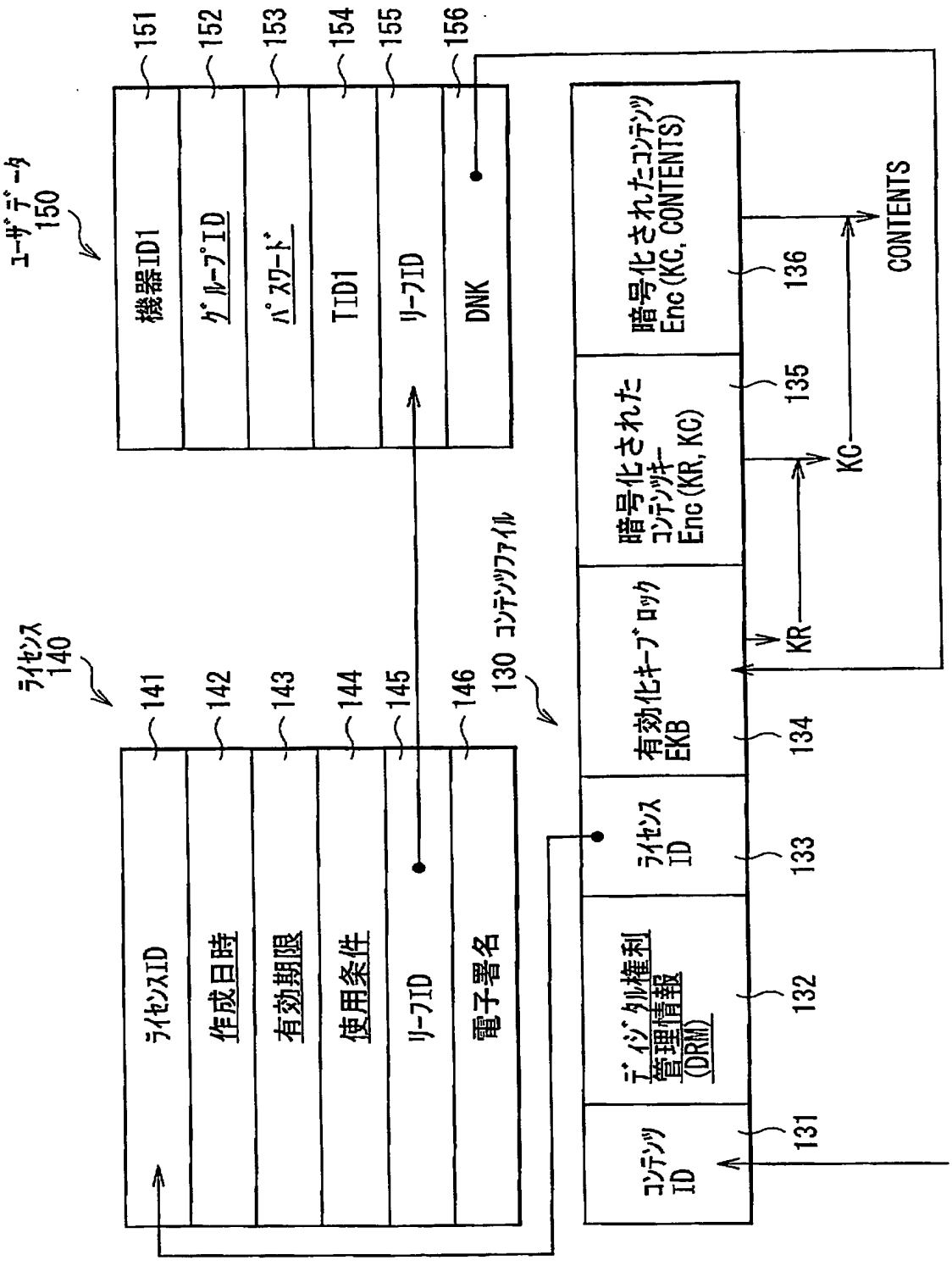
121 グループID	122 パスワード	123 グループ情報	124 機器ID	125 サービスデータ	
				リーフID	DNK
G0	ABCD	○○○○	D0	LF0	DNK0
			D1		
			D2		
G1	EFGH	△△△△	D3	LF1	DNK1
			D4		
G2	IJKL	××××	D5	LF2	DNK2
			D6		
			D7		
			D8		
⋮	⋮	⋮	⋮	⋮	⋮

(B)

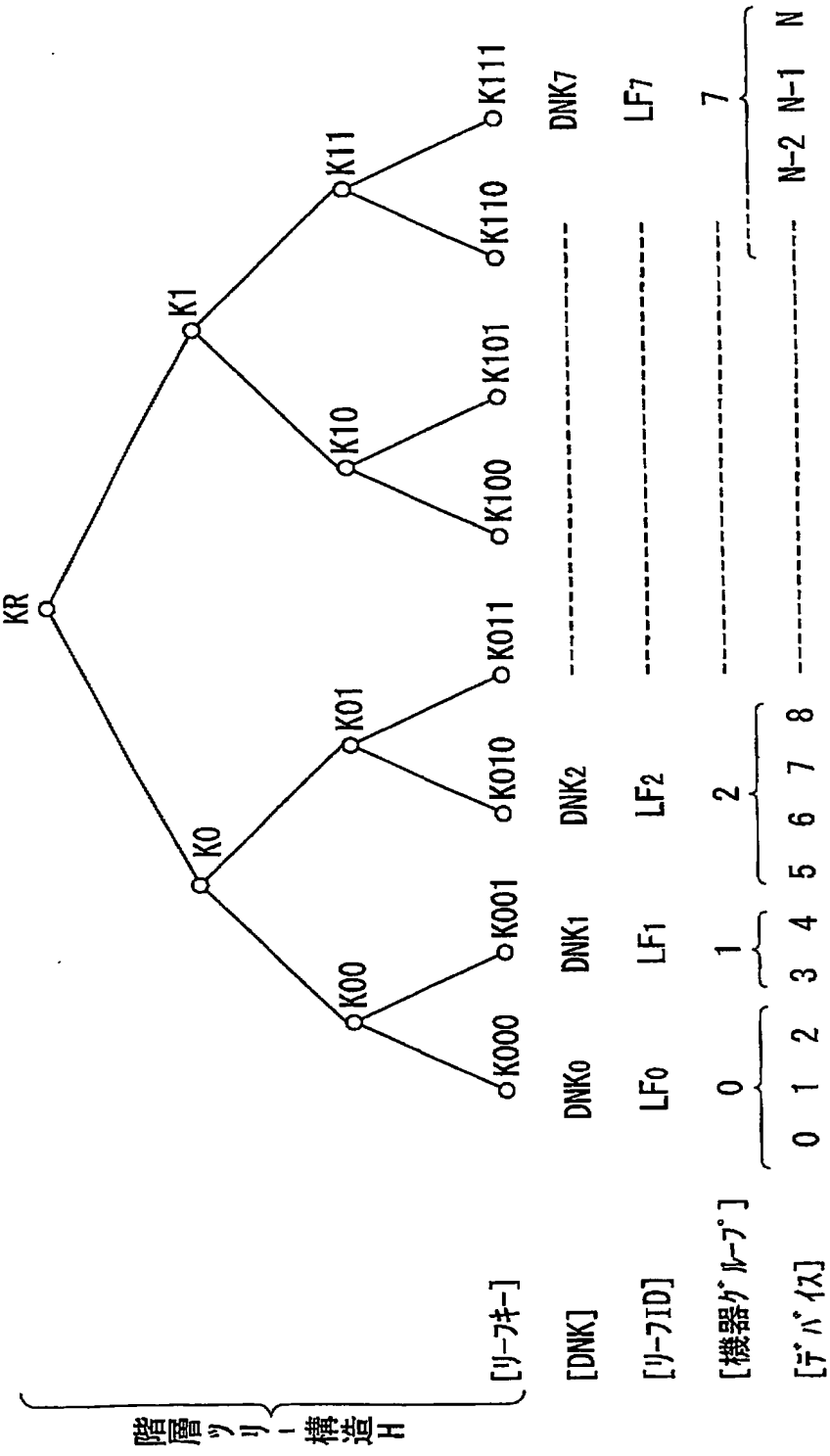
112 ライセンステーブル

127 ライセンスID	128 ライセンスの内容（使用条件等）	129 ライセンスしたグループのグループID
abcdef	○○○○□□□□	G0, G1, G2
ghijkl	□□□○○○○	G0
mnopqr	△△○○△△○	G1
stuvws	△△△△○○○	G1
stuvws	××××△△△	G2
⋮	⋮	⋮

【図６】


ユーザデータ
150
151
機器ID1
152
グループID
153
パスワード
154
TID1
155
リーフID
156
DNK
ライセンス
140
141
ライセンスID
142
作成日時
143
有効期限
144
使用条件
145
リーフID
146
電子署名
130 コンテンツファイル
131
コンテンツ
ID
132
デジタル権利
管理情報
(DRM)
133
ライセンス
ID
134
有効化キーブロック
EKB
135
暗号化された
コンテンツキー
Enc (KR, KC)
136
暗号化されたコンテンツ
Enc (KC, CONTENTS)
KR
KC
CONTENTS

【図７】


階層ツリー構造H
[リーフキー]
[DNK]
[リーフID]
[機器グループ]
[デバイス]
KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
DNK0
DNK1
DNK2
DNK7
LF0
LF1
LF2
LF7
0
1
2
7
0 1 2 3 4 5 6 7 8
N-2 N-1 N

【図８】

(A)　EKB=

Enc (K0, KR)
Enc (K1, KR)

(B)　DNK0=

Enc (K00, K0)
Enc (K000, K00)
K000

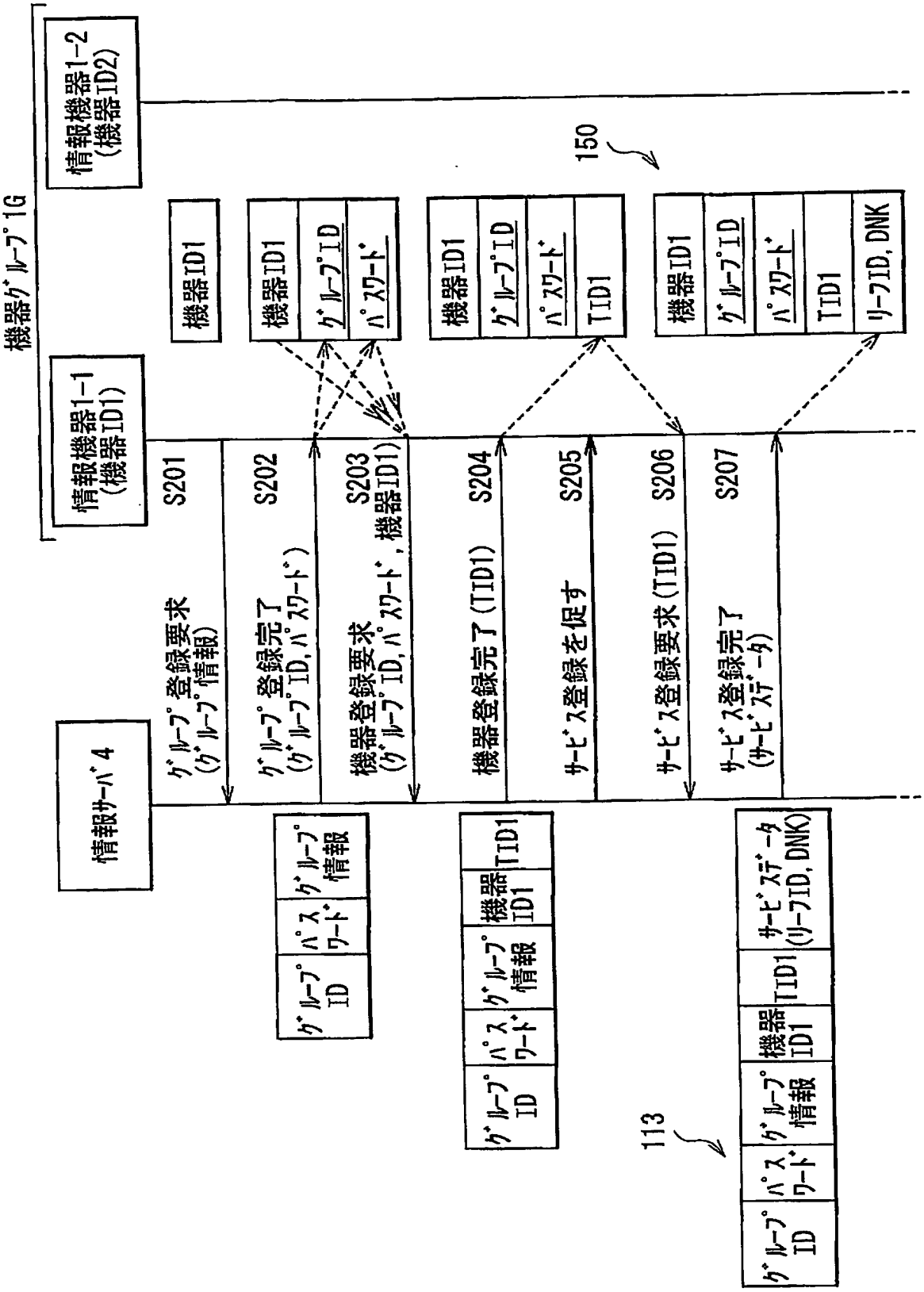
(C)　DNK1=

Enc (K00, K0)
Enc (K001, K00)
K001

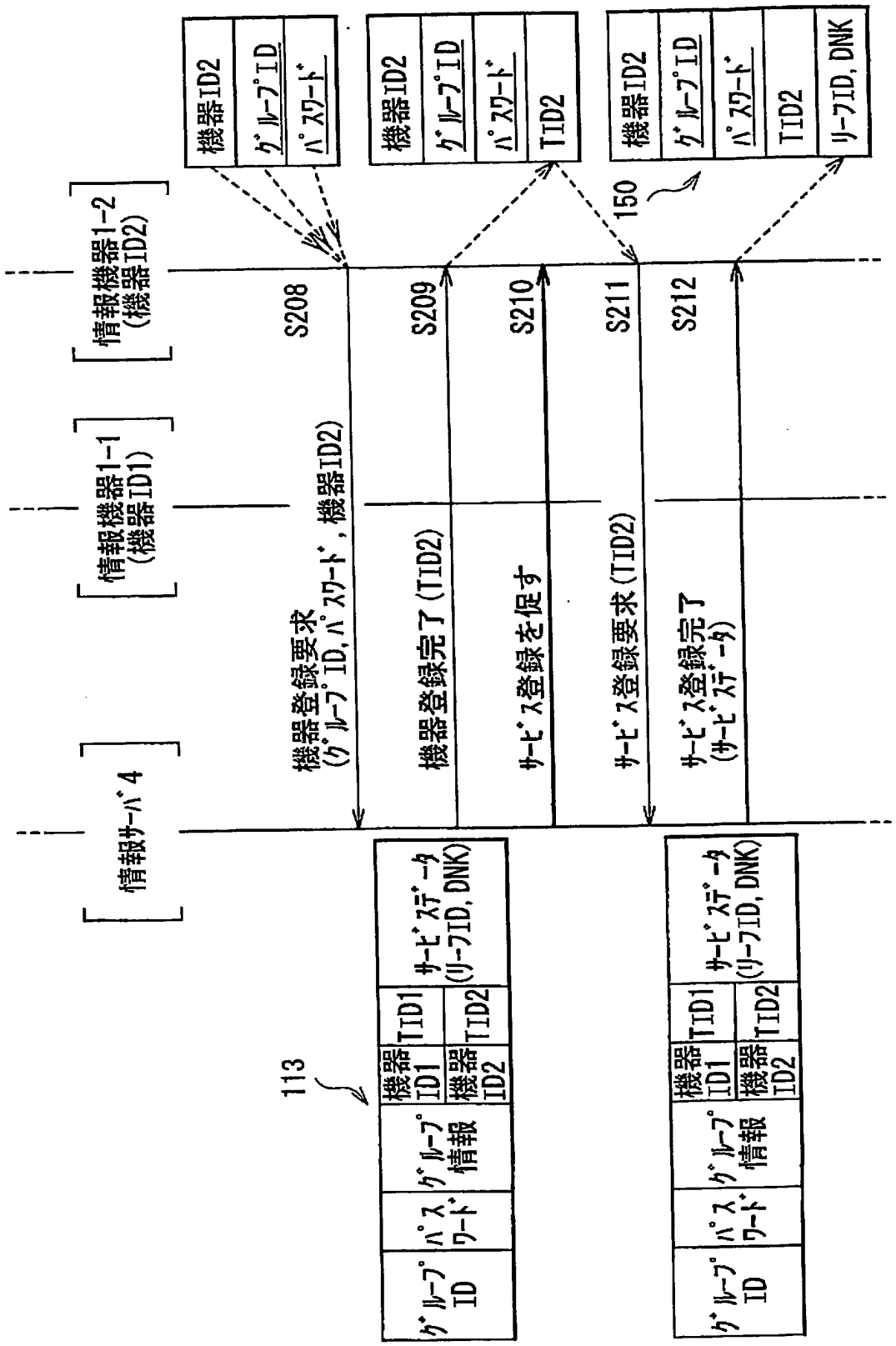
(D)　DNK2=

Enc (K01, K0)
Enc (K010, K01)
K010

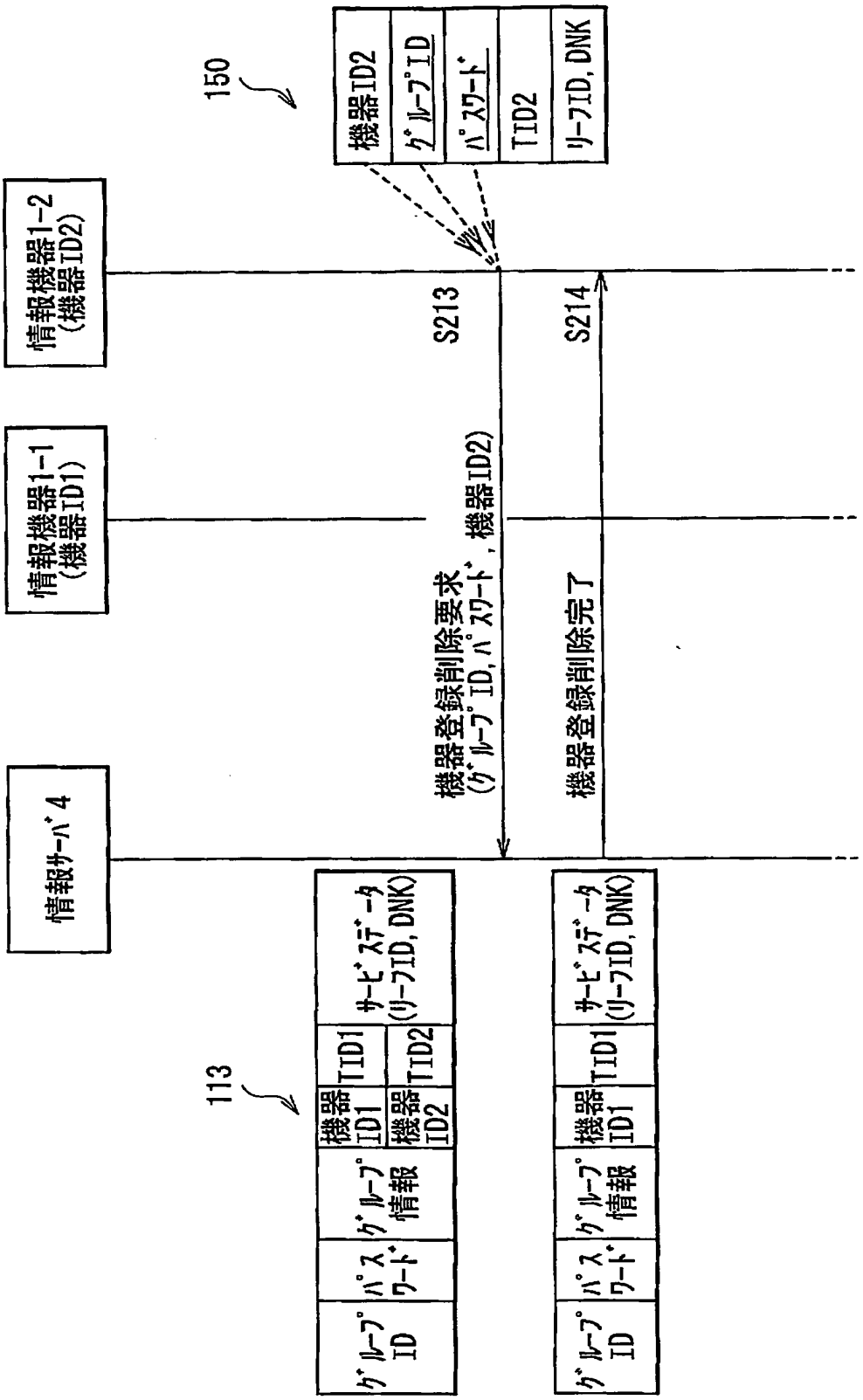
【図９】


機器ｸﾞﾙｰﾌﾟ1G
情報機器1-2
(機器ID2)
情報機器1-1
(機器ID1)
情報ｻｰﾊﾞ4
150
113
S201
S202
S203
S204
S205
S206
S207
ｸﾞﾙｰﾌﾟ登録要求
(ｸﾞﾙｰﾌﾟ情報)
ｸﾞﾙｰﾌﾟ登録完了
(ｸﾞﾙｰﾌﾟID,ﾊﾟｽﾜｰﾄﾞ)
機器登録要求
(ｸﾞﾙｰﾌﾟID,ﾊﾟｽﾜｰﾄﾞ,機器ID1)
機器登録完了(TID1)
ｻｰﾋﾞｽ登録を促す
ｻｰﾋﾞｽ登録要求(TID1)
ｻｰﾋﾞｽ登録完了
(ｻｰﾋﾞｽﾃﾞｰﾀ)
機器ID1
機器ID1 | ｸﾞﾙｰﾌﾟID | ﾊﾟｽﾜｰﾄﾞ
機器ID1 | ｸﾞﾙｰﾌﾟID | ﾊﾟｽﾜｰﾄﾞ | TID1
機器ID1 | ｸﾞﾙｰﾌﾟID | ﾊﾟｽﾜｰﾄﾞ | TID1 | ﾘｰﾌID,DNK
ｸﾞﾙｰﾌﾟID | ﾊﾟｽﾜｰﾄﾞ | ｸﾞﾙｰﾌﾟ情報
ｸﾞﾙｰﾌﾟID | ﾊﾟｽﾜｰﾄﾞ | ｸﾞﾙｰﾌﾟ情報 | 機器ID1 | TID1
ｸﾞﾙｰﾌﾟID | ﾊﾟｽﾜｰﾄﾞ | ｸﾞﾙｰﾌﾟ情報 | 機器ID1 | TID1 | ｻｰﾋﾞｽﾃﾞｰﾀ(ﾘｰﾌID,DNK)

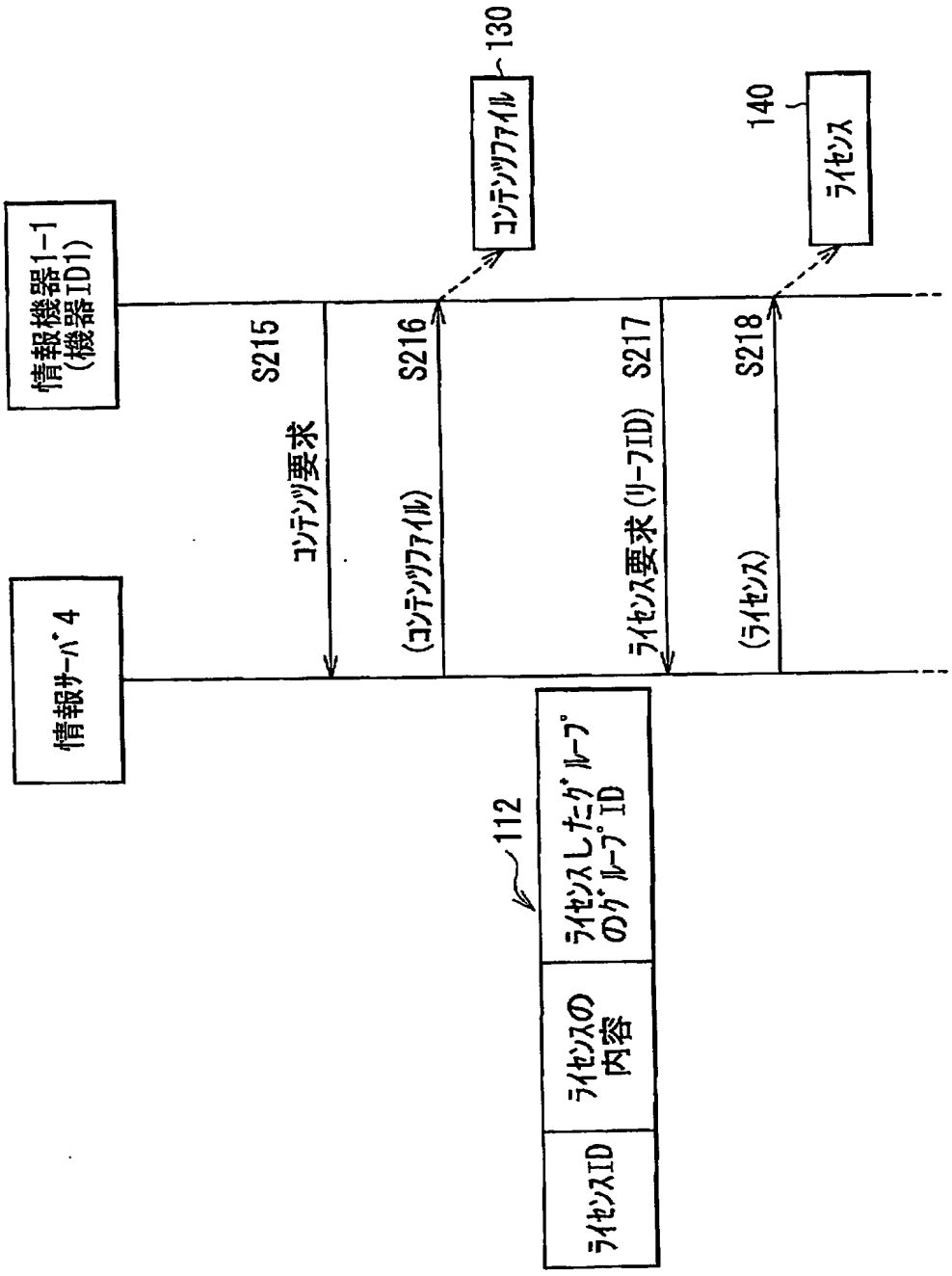
【図１０】


情報サーバ4
情報機器1-1 (機器ID1)
情報機器1-2 (機器ID2)
機器ID2
グループID
パスワード
TID2
リーフID, DNK
150
S208
S209
S210
S211
S212
機器登録要求 (グループID, パスワード, 機器ID2)
機器登録完了 (TID2)
サービス登録を促す
サービス登録要求 (TID2)
サービス登録完了 (サービスデータ)
113
グループID
パスワード
グループ情報
機器ID1
機器ID2
TID1
TID2
サービスデータ (リーフID, DNK)

【図１１】


150
機器ID2
ｸﾞﾙｰﾌﾟID
ﾊﾟｽﾜｰﾄﾞ
TID2
ﾘｰﾌID, DNK
情報機器1-2
(機器ID2)
情報機器1-1
(機器ID1)
情報ｻｰﾊﾞ4
S213
機器登録削除要求
(ｸﾞﾙｰﾌﾟID,ﾊﾟｽﾜｰﾄﾞ, 機器ID2)
S214
機器登録削除完了
113
ｸﾞﾙｰﾌﾟID
ﾊﾟｽﾜｰﾄﾞ
ｸﾞﾙｰﾌﾟ情報
機器ID1
機器ID2
TID1
TID2
ｻｰﾋﾞｽﾃﾞｰﾀ(ﾘｰﾌID, DNK)
ｸﾞﾙｰﾌﾟID
ﾊﾟｽﾜｰﾄﾞ
ｸﾞﾙｰﾌﾟ情報
機器ID1
TID1
ｻｰﾋﾞｽﾃﾞｰﾀ(ﾘｰﾌID, DNK)

【図１２】


情報機器1-1
(機器ID1)
情報サーバ4
S215
コンテンツ要求
S216
(コンテンツファイル)
コンテンツファイル
130
S217
ライセンス要求(リーフID)
S218
(ライセンス)
ライセンス
140
112
ライセンスID
ライセンスの内容
ライセンスしたﾀｰｹﾞｯﾄｸﾞﾙｰﾌﾟのｸﾞﾙｰﾌﾟID

【書類名】　要約書

【要約】

【課題】　コンテンツを正当な手段で入手したユーザが、そのコンテンツを、そのユーザ所有の他の情報機器でも利用できるようにする情報機器、情報サーバ、情報処理システム、情報処理方法および情報処理プログラムを提供する。

【解決手段】　情報サーバ４は、ユーザと、そのユーザの所有する情報機器１－１～１－３のそれぞれとを関連付けて管理し、同一ユーザの所有する情報機器には、同一のサービスデータ（リーフＩＤおよび鍵情報ＤＮＫ）を書き込むことにより、ユーザの所有する複数の情報機器を１つのグループとして扱う。この結果、ユーザ所有の情報機器１－１で取得したコンテンツを、ユーザ所有の他の情報機器１－２，１－３でも利用することも可能となる。また、情報機器１－１～１－３間で直接コンテンツやライセンスを移動するという方法により、それらの情報機器でのコンテンツ利用が可能になる。

【選択図】　図１

特願２００３－１６３９６８

出願人履歴情報

識別番号 [０００００２１８５]

１．変更年月日 １９９０年 ８月３０日
[変更理由] 新規登録
住所 東京都品川区北品川６丁目７番３５号
氏名 ソニー株式会社